The Cyber Security Social Contract

Policy Recommendations

for the

Obama Administration

and

111th Congress

A Twenty-First Century Model for Protecting and Defending Critical Technology Systems and Information

Board of Directors

Table of Contents

Overview of the Problem

The recent election was clearly a mandate for change. Nowhere is change more critically needed than in our nations approach to cyber security.

The Internet Security Alliance (ISA) strongly urges the incoming Administration and Congress to consider change in four major areas of cyber security.

First, there must be a substantially increased emphasis on, and investment in, addressing the serious and growing problems our nation, and our allies, face with respect to cyber infrastructure security.

The core protocols upon which the Internet was built are over 30 years old and were not designed with security in mind. Moreover, the explosion in mobile devices, based on the same insecure systems, has dramatically increased the ability to access the system for nefarious reasons.

Cyber security is no longer the domain of high school hackers but is populated by organized criminals, unfriendly nation states and terrorists. The problems we face are far more severe than compromised personal data. Our physical security is threatened by vulnerabilities in our electronic information systems.

Second, the needed investments in this system must be understood for what they really are; critical infrastructure maintenance and security.

More than $3 trillion dollars (a quarter of our nation's economic value) moves through the network every day. Virtually every element of out nation's activity including defense, finance, communications, energy, manufacturing etc. is now reliant on these electronic systems.

For a century both foreign and domestic capitol flowed into the US because the US was understood to be a safe place to conduct commerce. The growing vulnerability in our cyber systems threatens to undermine that confidence.

It is now a national priority to develop a low carbon, green economy by investing in clean infrastructure. Electronic commerce is the ultimate clean technology. However, even universal broadband access, without security will not achieve this goal. If the US can become recognized as the world leader in cyber security we can gain short and long term economic, environmental and other advantages.

Third, the fundamental orientation toward cyber security needs to change. Cyber security is not (solely) an "IT" issue. It is an enterprise wide risk management issue.

Indeed the most common avenue of cyber incursions is through insiders who have the electronic keys to the system. To attempt to address cyber security without appreciating the economic, legal, human

resource, communications, as well as the Information Technology aspects is to fundamentally misunderstand the issue.

Forth, government and industry must develop a much more thoughtful, fundamental and contemporary relationship to address their mutual (not just government's) cyber security needs.

Neither the laissez faire approach of the Bush Administration's National Strategy to Secure Cyber Space nor a system of federally determined mandates are likely to succeed in accomplishing our goals.

Government Must Embrace Some Inconvenient Truths

First, is that the diversified nature of the internet places much of the critical national security operations in private industry's hands. This does not mean government has a lesser role, just a different, and frankly 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 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.

Industry and government must construct a mutually beneficial social contract which addresses, creatively and pragmatically, the security of our cyber infrastructure.

The good news is that we actually do know a great deal about how to construct strong cyber systems. Experts and independent research have continually reported that by following identifiable security practices between 80 and 90% of attacks can be thwarted. Our first task needs to be providing the incentives for people to do what we already know can work to substantially curb this massive threat.

With a coherent strategy we believe substantial progress can be made in this area fairly quickly. However, it will require the three conceptual changes articulated above.

The Cyber Security Social Contract

A social contract is essentially a deal between industry and government wherein both entities agree to provide services and receive benefits resulting in a larger social good.

The social contract ISA is proposing is based on the agreement between government and the utilities in the early 20th century which had the goal of providing universal phone, power and light service to Americans. That model worked.

In the early 1900s the government realized that there would be enormous public benefits to universal utility service ranging from economic development to enhanced public safety. Policy makers understood that much of the needed infrastructure development would be undertaken thanks to the market incentives inherent in providing these services. However, government also realized that these natural market incentives would not extend to the entirety of the population. Moreover, policy makers realized that it was completely impractical for the government to either fund the infrastructure enhancements needed for universal service themselves or simply mandate that it be done.

In an enlightened and pragmatic move, government struck a deal with the utilities. The utilities guaranteed to make the infrastructure upgrades necessary to provide universal service. In return government essentially guaranteed a return on the required private investment economically sufficient to make the investments good business decisions. The utilities maintained the investments over time because they were also provided exclusive franchises for the service area.

In this instance government harnessed the power of private investment to achieve vital social goals, which had the added benefit of stimulating greater economic growth. Meanwhile consumers were protected by the requirement to provide service at government regulated rates. A similar model can be developed for cyber security. The necessary infrastructure improvements, technical and otherwise, can be addressed through incentives for private investment while the cyber related consumer protection items (SPAM/personal identity) are addressed by regulation.

While not identical, the parallels with respect to cyber security are striking. As with public utility service, cyber security cannot be provided directly by the government. As with utility service, many companies do an excellent job with information security as required by their business plans. As with public utility service, the inherent market incentives are insufficient to provide the breadth of security required by the public's compelling national economic and security interests.

Since a voluntary system will not provide adequate market incentives to accommodate the public interest, and due to the global nature of the Internet, a federally mandated system will not work either. A social contract wherein government provides incentives for the private sector to make cyber security investments that are not justified by current business plans is a pragmatic alternative.

This report will outline what the Internet Security Alliance Board of Directors believes are the most serious problems facing the nation with respect to cyber security in several critical sectors. It identifies what the government can best do, both long and short term to address these needs and specifies a series of steps the new Administration and Congress can take toward establishing a coherent, pragmatic, effective and sustainable system of cyber security

Why the Internet is Different

The Internet is arguably the most transformative invention since the printing press. It is unlike anything we have dealt with before. As a result, managing the Internet will require an equally revolutionary approach to industry government cooperation.

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" to which we have applied a common noun. The independent networks are knitted together -- some public, some private -- all transmitting information across corporate and national borders without stopping to pay tolls or check regional sensitivities.

One of the most common misconceptions about Internet security is that it is a technical problem. It is not. To address Internet security as a technical issue without simultaneously addressing the economic, human resource and other risk management issues is to fundamentally misunderstand the issue.

Why the National Strategy Is Not Working

The Bush Administration's 2002 National Strategy to Secure Cyber Space advocated a market-based, voluntary approach to industry cyber security. ISA supported that philosophy, but has always maintained that the "missing link" in the National Strategy is the lack of an incentive program to bridge the gap between security investments that industry would make for their own corporate needs, and the additional investments required to accommodate the broader national interest.

The Administration's 2006 National Infrastructure Protection Plan acknowledged this gap exists, however no serious attempt to construct the needed incentives for additional private investment in cyber security have been made.

It is now apparent that the approach in the National Strategy has not worked sufficiently. Research documents that a purely voluntary approach is insufficient.

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 parties use of their data

In short 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.

Why Regulatory Models Won't Work

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.

Among the reasons 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 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 affect
➢ 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 legislatively wasting valuable time

The Good News – We Do Know What Works

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 breech 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. It concluded that in 87% of cases investigators concluded 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.

Core Components of the Cyber Security Social Contract

Successive chapters of this report and the appendix provide specifics as to components that may be included in the program we are referring to here as the *cyber security social contract*. Naturally with the diversity of the private sector there will never be a single document that comprises all the varying relationships. However the contract, as a conceptual framework, would include the following core elements:

Identifying Government's Role
- ➢ Policy makers must first educate themselves better with respect to the Internet and its role in modern American society
- ➢ Government must get its own house in order
- ➢ Policy makers must establish a program to educate others
- ➢ Government must create incentives for industry to invest in cyber security beyond what is necessitated already by corporate business plans
- ➢ Government must address the serious 10% of high value threats
- ➢ Government must support the necessary R&D to address issues for which there is not an industry value proposition
- ➢ Government must, with industry, overcome the historic obstacles to practical timely, actionable information sharing

Identifying Industry's Role
- ➢ Continue to develop verifiable standards and practices that will continually strengthen cyber security
- ➢ Develop technology that will meet consumer and government needs with security systems baked in
- ➢ Implement best practices and standards required to secure their networks
- ➢ Use their businesses to expand the perimeter of security through contracts
- ➢ Work with government to develop a practical exchange to effectuate the cyber social contract
- ➢ Work with government to overcome information sharing barriers

Identifying Incentives for Businesses that Implement Industry Best Practices & Standards
- ➢ Congress can use its market power by more prominently including security, along with cost into its procurement process
- ➢ Congress can lead by example by making federal agencies secure
- ➢ Congress can expand the SAFETY Act to address cyber security
- ➢ Congress can stimulate the stunted cyber insurance marketplace
- ➢ Congress can adapt the Sema-Tech model to cyber security
- ➢ Government can create "Baldrige" style awards programs
- ➢ Congress can provide civil liability protection to good actors
- ➢ Congress can provide Stafford Act relief for good actors
- ➢ Congress can provide tax incentives or SBA loans for small companies to address cyber security issues
- ➢ Congress can enhance information sharing based on mutual industry cooperation

Banking and Finance

What are the greatest problems your company (or industry sector if you prefer) perceives regarding cyber security?

1. The lack of software quality or assurance in the products we use within our tech infrastructure. There are simply too many vulnerabilities out there to exploit; this is the underlying heart to most of the problems we face. It allows hackers, criminals or nation states to attack the confidentiality of our information or even the integrity of our information. From a public policy perspective, everyone reaps some of the benefit of investment in cyber security by a single company. This free-rider aspect makes other companies less likely to improve their own security. Similarly, insecure software and hardware may impose some of their cost on the public at large rather than the manufacturer or purchaser. Thus these products, from the public perspective, may be under-priced and over-consumed relative to their true risk to the general public.

2. We lack the proper incentives structure to address the information security issues. For too many corporations, simply "fear motivation", whether the result of a regulatory environment or the theoretical potential financial impact of a major cyber event is insufficient to adopt desired loss mitigation and prevention actions. This is especially troublesome given the interdependent nature of the internet where the failure of one institution can rapidly have adverse consequences on other, even better protected, institutions. The mix of positive and negative incentives must be realigned.

3. We do not have a common risk framework that helps organizations to understand all the various risks that a cyber security incident represents such as financial reputation, regulatory, legal, compliance, revenue etc. and which provides a roadmap for how to maximize ROI on cyber expenditures using an enterprise risk management paradigm. From a corporate perspective, while banking and finance sectors have been more proactive and forward thinking as well as far more advanced than most sectors, cyber security is still perceived too often simply as an IT cost center rather than as an enterprise wide risk management issue with serious financial implications. The silo specific view of cyber issues, fueled by antiquated corporate structures and attitudes results in an insufficient analysis of the true needs and values associated with cyber security.

4. There is an inability to purchase sufficient insurance. As is common with any new type of insurance, most carriers are reluctant to take the chance of assuming new and untested risks with uncertain returns. This is especially the case when too many institutions see cyber-risk as a fundamental IT issue (See Problem 3) and therefore don't even think about insurance thereby depriving insurance carriers of the necessary "spread of risk" to make premiums more affordable and coverage limits higher. Yet, the public policy necessity for a robust and functional private insurance system is overwhelming. Insurers have a strong financial self-interest in greater security and their requirements are continually increasing. Insurers require some level of security as a pre-condition of coverage, and companies adopting better security practices receive lower insurance rates. Thus, insurance helps companies internalize both the benefits of good security and the costs of poor security.

In addition, with widely adopted insurance, the requirements to get coverage become de-facto standards. These de-facto standards can be updated as necessary, and far more quickly, than those generated through the traditional government regulatory mechanisms.

In addition to motivating continually improving security, insurance is enormously beneficial in the event of a large-scale security incident. Insurance can provide a smooth funding mechanism for recovery from major losses helping businesses to return to normal and reducing the need for direct government assistance. Finally, insurance allows for risks to be fairly distributed with higher premiums for companies whose expected loss from cyber risk is greater. This avoids potentially dangerous concentration of risk while also preventing free-riding.

What are the biggest obstacles you perceive in addressing the major problems related to cyber security?

1. Lack of Software Quality: The lack of an effective mechanism to motivate technology providers, not just IT and telecommunications companies, but others like the financial services industry to assess their security. We need to find ways to motivate any company that provides technology products to test their products adequately, assure secure coding practices, identify all the possible threats to that product and build into the product itself the necessary security.

2. Lack of management incentives: Virtually every corporation in America has by now integrated the wonders of digitalization into their business plans via web-based sales, employee efficiency, supply chain management, advertising, etc. However, security in general, and cyber security in particular, is still regarded as a corporate cost center to be minimized rather than a foundational corporate asset that needs to be strengthened and maintained to support sustained profitability. In order to change this dominant, corporate perception, visionary leaders must become more engaged in managing their corporate structures to assure that proper incentives for enterprise wide security are in place.

Public policy makers can provide major assistance in this effort by educating themselves as to the nature of the modern information system referred to as cyber space, or the Internet, and crafting a new approach to industry/ government relationships based on a market based global model rather than the sector specific regulatory model developed two centuries ago and still largely in existence today. One example of such an incentive based partnership would be the creation of a "cyber Safety-Act" which would provide incentives to create and maintain cyber-risk technology, processes and procedures much like what the Safety Act does now to encourage the creation and maintenance of anti-terrorism technology.

3. Lack of Multi-departmental coordinated roadmap: Modern corporations are inherently integrated by modern technology. Yet unfortunately, corporate structures and decision making has largely retained a 19/20th century model of independent departments and silos which do not facilitate appreciation of the interdependency that is a corporate fact of life. To date, there has not been a practical methodology developed which corporations can easily use that addresses the risks and potential financial losses created by the lack of appreciation of this interdependency.

Corporations need to truly understand the financial impacts of insufficient cyber security. In addition, they need to enact management systems, directed by their CFO's which bring everyone to the table and address cyber security issues on an enterprise-wide basis. It would involve security and technology personnel, but they would not be in charge of cyber risk management. An enterprise-wise structure

must include at minimum, financial, legal, operational, human resources, communications, public policy, investor relations, compliance, risk management and senior corporate officials.

One such roadmap created by private industry in October 2008 by the American National Standards Institute and the Internet Security Alliance at the request of the Department of Homeland Security called "*The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask*" provides such a roadmap.
(Available as a free download at -http://webstore.ansi.org/cybersecurity.aspx)

4. Lack of Insurance: We need a better understanding of the need for, and role of, insurance. Despite the public policy benefits of cyber insurance, the market has been truncated by several problems. These include the fear of large losses from cyber hurricanes. The uncertain risks are difficult for insurers to plan for and provide upward pressure on premiums making the take rates lower than is in the public's interest. In addition, the lack of good actuarial data, largely due to under-reporting of cyber events makes properly quantifying risk difficult, which also provides upward pressure on rates. Normally, insurers purchase reinsurance to mitigate against very large losses by diversifying risk globally. Cyber risk, however, has a significant international component making it more difficult for re-insurers to avoid risk concentration.

The solution to this problem is three fold. First, educate owners of critical infrastructure of the need to incorporate insurance as a risk management technique in the analysis of cyber-risk in much the same way as they do with respect to fire, flood and other physical risks. Second, assist in R&D activities for both buyers and sellers of insurance so that accurate industry actuarial tables can be created as quickly as possible. Third, reduce by way of appropriate public-private partnership measures the short term risk and fear of insurance carriers that a "cyber-hurricane" early in the product cycle would cause to long term profitability and therefore that it isn't worth entering the market thus removing the obstacles to creating an insurance market.

What can the US Government do to best assist you in improving your cyber security in the short term?

1. Educate itself.

Government must immediately begin to educate policy makers as to the true nature of the technology and the problem we are facing, and the need to address it through a 21st century designed solution.

It is well known that too many policy makers treat information technology as a specialized subject matter that they have no need of understanding in order to pass legislation on. This attitude must be changed dramatically.

While there is no need for policy makers to learn how to program or configure their own computers, they must educate themselves regarding the policy implications that this fundamental and ubiquitously deployed system has on virtually every aspect of modern public policy. Unless they undertake this fundamental self-educating experience, the prospect of ill-founded law and policy will remain unnecessarily high and cause great risk to the nation.

2. Educate the providers of the systems.

 The federal government should to put together a broad and detailed communications plan to make technology providers aware of the cyber risk threat and identify some steps or actions that they, the providers, can take to mitigate some of this risk in the short term. The provider community needs to be more aware of the issues users face and aware of the security controls that they should employ in the products they build.

3. Educate the purchaser of systems as to the need for a true enterprise risk management approach to cyber-security.

The federal government, working with private industry, should put together a broad and detailed communication plan to make corporate internet users aware of the cyber risk threat and identify the types of financial losses that can be suffered as well as the mitigation actions that should be evaluated in all departments of the company, both IT and non-IT related.

4. Become a model for the rest of society.

The annual FISMA scores reported by government agencies are disheartening, and at this stage embarrassing.

Government must begin by getting their own cyber house in order. Clearly, this is necessary before they attempt to direct the private sector as to how they ought to secure their cyber systems.

Immediately, the government can better use its own market power to model good security purchasing and help drive down the costs of cyber security application. For example, the government can mandate that companies that hold government data or access government systems have the proper technology, process, procedures and insurance in place.

Government can immediately provide better training for its own work force on security management and begin to incentivize, at the individual level, the adherence to good security practices.

Government can immediately undertake dramatically increased funding of cyber education to assure that the US workforce is better prepared to defend our cyber infrastructure. They can also work with colleges and universities to build awareness into their curriculum so people who go through IT and computer science training come out grounded in the full range of security issues, from both technological and economic perspectives.

Government can immediately increase funding for research and development for cyber security technologies benefiting the entire system, such as modern protocols. This much needed R & D is unlikely to be done by the private sector because its application and implementation does not drive individual corporate business plans although it does benefit the collective.
Government can immediately begin to treat the private sector like full partners in generic cyber security. While the partnership model articulated in the National Infrastructure Protection Plan is basically correct, the implementation of the partnership model has been inadequate. Too often the government has insisted on maintaining the role of 'senior partner", and relegated the private sector to

the role of stakeholder". The failure of the government to adapt to a more modern understanding of the appropriate roles and responsibilities it must take in the public private partnership results in a lessening of needed trust and cooperation which results in vastly reduced national cyber security.

What can the US Government do to best assist you in improving your cyber security in the long term?

Government needs to work with private industry to architect and design a secure technology infrastructure from the ground up. The infrastructure should include secure hardware and operating systems network devices and Internet services.
Government needs to rethink its role in global cyber security and aggressively engage with the multiple partners. It must work with in a 21st century, market based program to address cyber needs on a practical, sustainable, dynamic and effective basis.

At the core, government must take the many market incentive programs it has traditionally used in other sectors of the economy such as energy, agriculture, ground transportation, aviation and environment and begin to apply these principles to the cyber security issues it faces.

The National Strategy to Secure Cyber Space, while well intentioned in its market orientation, was inadequate in advocating a completely voluntary model. Such a model, while accurate in many corporate situations, does not have the expanse needed to address the broad-based issues in cyber space where the weak link in the chain can break the entire security perimeter.

Government must utilize a multi-layered approach that applies regulation where appropriate, such as in consumer protection, with market incentives, which can respond to the fast changing threat sectors faster, more effectively and more broadly than a traditional regulatory model can accommodate. Among the incentives government needs to investigate and apply to enhanced cyber security are:

- ➢ Procurement
- ➢ Stafford Act relief
- ➢ Cyber Safety Act
- ➢ Streamlined compliance of multiple regimes (SOX/HIPPA/GLB etc.)
- ➢ Tax incentives (especially for small businesses)
- ➢ Anti-Trust relief
- ➢ Insurance benefits (flood and crop insurance models)
- ➢ Awards programs
- ➢ Cost shared R & D projects
- ➢ R & D tax credits and incentives for conducting R & D

If you had 5 minutes to discuss cyber security with President Obama what would you tell him?

Mr. President, the threats to our infrastructure from cyber attacks, whether from domestic or foreign based, cannot be successfully defended or mitigated against using our current paradigm of thinking. Specifically, we need:

1. Better software quality or assurance in the products we use within our tech infrastructure. To accomplish this, we need to find effective mechanisms to motivate technology providers to assess their security and increase the quality of product security.
2. Better positive based incentives to mix with existing negative or classic regulatory based incentives to adopt best practices. To accomplish this, we can look at historical examples of positive incentive programs, such as the Safety Act, and apply such examples to the cyber-risk problem.
3. Educate both providers and users of technology of the need for a complete enterprise risk management approach to cyber security. To accomplish this, the public and private sector should work together to create an effective communication strategy which provides education directed to the chief financial officers of the nation on the potential financial cost of inadequate cyber security and a roadmap on how best to address those risks from both an IT and non-IT viewpoint.
4. Have a robust insurance market which can provide terms, conditions and limits of liability which will both encourage the adoption of best practices by way of adjusting the affordability and availability of insurance as well as provide an efficient funding mechanism in the event of a massive cyber-event. To accomplish this, the public sector should partner with the insurance industry in educational campaigns, research as well as aligning public based incentives (see 3 above) with insurance based incentives.

Communications

What are the greatest problems your company (or industry sector if you prefer) perceives regarding cyber security?

Some companies are ahead of the curve. We have invested in technology and personnel and have established governance structures that look at cyber security from the bottom up in each business unit and from the top down through corporate policy and compliance efforts. We continually audit and assess how we are doing. We also aggressively reach out and partner with government; both when we serve them as clients and on a public policy level.

However, too many of the companies we provide service to don't realize that cyber security is a requirement in systems we deploy. Although there is a significant risk present today, they don't look at cyber security as a necessary element of investment, it's an after thought. Even some organizations that do realize there is a threat, don't realize the magnitude.

We live in a hyper connected world where every "node" affects every other one, and the weak links in the chain endanger everyone. The people who do get it are burdened with the costs for those who don't. Hence, we need a program that will reach everyone. People often don't get that they may have secured a portion of the network but they are still vulnerable. The lack of awareness and the need to be constantly thinking about this is a major problem

This includes all levels of government from the highest to the lowest levels. We worry if we fully understand the needs of our clients especially our government agency clients.

Even companies who are on top of the problem have concerns. We worry about the IT supply chain. We worry about the off-shore security of both employees and equipment. We worry if we are staying ahead of the emerging threats. Are we fully appreciating the link between physical and cyber security?

From an "all hazards" approach, we worry about the overall architecture of the system. If there were a major incident in one facility, will we and our customers have what they need to survive a major hit? This is especially worrisome in the government enterprise sector.

We worry about SCADA attacks because we are dependent on the power supply to provide the services we are responsible for in an attack.

And, we worry about what it is that we do not yet know.

What are the biggest obstacles you perceive for your company (or industry sector) in addressing the major problems related to cyber security?

For companies who have already made cyber security a corporate priority, we need to be sure that the policies and programs in place are being implemented both internally and externally with our partners.

The terms and conditions on the network contracts need to be structured to make sure we have the right agents in place and specify the roles and responsibilities to make sure we have adequate back up systems.

Since we are concerned about the insider threat, we need to be sure the background checks are fully informed. To the degree we are working with our government clients, does government have the data needed to make sure our systems are properly secured and are they sharing that data appropriately?

The supply chain issues also create obstacles. We need to test and screen equipment we get from our vendors. This means we need to have a secure and trusted relationship with these vendors and that they are following through properly.

There also needs to be appropriate training especially for people involved in these issues overseas. Do we have the right policy regarding the use of our equipment overseas? Have we addressed the cultural issues so that we understand security the same way our overseas partners understand it? Are we all on the same page?

For organizations that have not yet made cyber security a true priority there are other barriers, often primarily economic.

There is a tremendous commoditization taking place in the industry. This means more and more features are being included in more and more products so there is very little margin to cover the cost of security in the product.

This dwindling economic margin means that research and development cannot be performed to assure that there is an adequate degree of security in the product.

Organizations need to develop a greater awareness that the threat is real, and they may have to pay to address it. This is very difficult t in a commoditized market wherein users are not placing a high value on security.

The market reality is that we want more and more features. If the customers don't think it's important for a feature to be secure, or are uninterested in paying for that security, we have a problem.

When the consumer doesn't demand security and is unwilling to pay for it that makes providing security uneconomic. As a result, they don't have the demand needed for a trickle down economics.

There just are not adequate economic incentives there for security. There is a phenomenal lack of incentive for cyber security spending.

What can the US Government do to best assist you in improving your cyber security in the short term?

Again, starting with the organizations that already have established a priority on cyber security, we need better intelligence and information sharing for these organizations.

We need to make sure the right channels are in place and approved by the lawyers. Attempting to address the information sharing issues between industry and government without involving the lawyers reflects a misunderstanding of some of our core problems and will lead to the same frustration we have had addressing this issue for years.

We need to be sure that the information being shared by our government partners can be put into action. We need to get the road blocks out of the way with respect to the timeliness of the information

With the roll out of the cyber initiative, we need to be able to move forward quickly to implement good ideas and encourage voluntary steps instead of federal mandates, which due to the inherent nature of the Internet will not work.

Government needs to work with industry on establishing standards and practices that appreciate the evolving nature of multi-media communication technologies such as VoIP to help assure that this and other modern platforms are properly secured.

For organizations that are focused on the threat, and even more urgently for those who have not yet come to the realization, there needs to be serious education across sectors about the threat. Educational efforts must be far, far more aggressive than what has existed so far. There was a lot done after 911 to educate about terrorism in general. We need a similar education initiative with respect to cyber security.

Government needs to embrace the idea that cyber security is a business issue not a technical issue. Again, this needs to be done much more systematically, aggressively and with more sophistication than previous programs.

The government needs to examine how it can use its market powers, not its regulatory powers to motivate an ongoing and sustainable system of cyber security. There are wide ranges of ways government can begin to do this.

Among some of the possible examples worthy of consideration:

 ➢ Security can be better tied into government procurement with higher levels of cyber security necessary to get government contracts.
 ➢ The government should work with the finance and insurance industry to incorporate cyber security risk management as an underwriting principle. Adopting a risk management framework is the only way we will achieve sustainable cyber security among the organizations that own and operate the vast majority of what we call the Internet.
 ➢ The Small Business Administration (SBA) generates a lot of loans to new and expanding businesses and this process could be used to encourage better cyber security practices.
 ➢ ISA has testified before Congress on many occasions specifying other mechanisms for providing market incentives (see detailed appendix).

What can the US Government do to best assist you in improving your cyber security in the long term?

 ➢ There needs to be Research and Development; especially in areas such as the development and implementation of new secure basic protocols for the Internet, which will not be undertaken in the private sector due to the lack of a viable business plan for implementing them profitably.

- Government needs to be involved in supply chain issues and support solutions that are economically practical for the private sector. This would include working with the private sector to develop a consensus framework to assure secure systems. This needs to be done on an international basis with market motivators that transcend national boundaries.
- Involve American business schools by making cyber security educational programs a domain of expertise and integrating cyber security into undergraduate and MBA (or even liberal arts) courses.
- Loans need to be made available and procurement reform must be addressed.
- Make sure non-defense and intelligence (civilian agencies) sectors of the government make cyber security a priority.
- Re-examine laws governing telecommunications from the 1980's to assure they allow for appropriate security in the digital age.
- Examine the legal structures to encourage voluntary reporting of security incidents and reasonable data gathering that can be used to properly assess risk on a corporate basis.

If you had 5 minutes to discuss cyber security with President Obama what would you tell him?

- There is a tremendous awareness problem with respect to cyber security.

- We need an incentive model to encourage better cyber security.

- We need to drive home the idea that you can have 95% security but the other 5% is still a massive hole. There is not enough of an appreciation of this at higher levels within government today.

In short:

1. Be careful as you craft policies and expectations.
2. Be knowledgeable about what industry is doing before you act.
3. Embrace the partnership model; not mandates.
4. Advocate for adequate funding for R & D.
5. Make sure intelligence is well coordinated with industry.
6.

Defense Industrial Base

What are the greatest problems your company (or industry sector if you prefer) perceives regarding cyber security?

The most pressing cyber security issue facing defense industrial base (DIB) companies is a near existential threat from state-sponsored foreign intelligence services (FIS) who possess the capability to establish deep and persistent access to our networks, accessing sensitive intellectual property (IP) that has long term negative implications for US national security.

The current technologies are woefully inadequate. They can deter the average script kiddie but provide little defense against foreign state sponsored attacks and espionage, which represent 5% of the threat responsible for some of the most serious damage. Signature-based intrusion detection, firewalls, and anti virus technologies are all deployed, but they do little to identify or prevent more sophisticated adversaries.

We are responsible for protecting against physical, cyber and economic attack – the unique solutions we provide are a top target for cyber and nation state sponsored cyber crime.

DIB member networks are routinely exposed to hostile intelligence collection as a result of our adversary's ability to exploit end users and basic network vulnerabilities to gain deep access to proprietary networks

The fundamental problem the defense industry, and perhaps all industries face, is the inherent anonymity of the internet. Almost all our most serious problems stem from the fact that it is too easy to disguise your identity and location. Spam, spoofed e-mail addresses, multi-hopping exploits, and third party domain registration all serve to make internet crime and intellectual property theft all but impossible to prevent. To date, little has been done to raise the costs to the adversary for perpetrating cyber-based crimes against this country's industries and government.

What are the biggest obstacles you perceive for your company (or industry sector) in addressing the major problems related to cyber security?

DIB member cyber security operations are largely ill-equipped to discriminate between professional intelligence operations, competitor collection efforts, and common criminal activity on their networks. Many network operations centers remain oriented toward signature-based detection schemes designed to counter threats over a decade old.

➢ Most DIB members lack the expertise to accurately determine who is targeting them, what information is at risk, and how these entities are accessing and exfiltrating their most sensitive information.

- The detailed second and third phase all-source intelligence analysis necessary to fuse technical cyber-indicators with broader, non-technical threat intelligence typically falls into an ill-defined area of responsibility between physical and information security departments for DIB organizations. The result is little effort devoted to this critical all-source analysis that can give meaningful context to the threats they face.

- Many DIB organizations are being daily penetrated — often with little awareness — by highly sophisticated, professional state sponsored groups and other experienced organized criminal operations using custom-designed tools that enable them to perform detailed network reconnaissance and data exfiltration at will.

- Consequently, most DIB member information security professionals, faced with limited budgets and junior personnel, are locked in a reactive defensive posture. This position allows for little more than signature-based perimeter monitoring and — if detected — malware eradication as an operating paradigm against professional foreign intelligence operations tasked with penetrating, surveying, and exfiltrating specific sets of information.

This is not a problem any single company can address. We can invest a great deal of time and money to treat the symptoms (detect and respond to incidents), but only the international internet community can begin to address the problem. The erosion of this nation's R&D capabilities will continue until a comprehensive US national policy is developed — and worked in concert with the international community — to identify conclusively those nation-states or other entities providing explicit or tacit support to groups targeting the US, the problem will continue unabated.

What can the US Government do to best assist you in improving your cyber security in the short term?

We believe this is an intelligence war and that the most pressing issue is the theft of our intellectual property, which has major national security implications

The US Government needs to generate and share with the private sector an operational understanding of how adversaries create and exploit our cyber vulnerabilities, disclosing the extent and reach of the adversary's capabilities. DIB members need timely, actionable information regarding our adversaries' collection targets to better secure sensitive intellectual property and to ensure future competitiveness against both domestic peers and new foreign entrants into this market space.

- Many foreign intelligence services support their commercial sector as a core mission; an activity which the US Intelligence Community is prohibited from performing. DIB member companies urgently need more timely support from US counterintelligence agencies when they identify ongoing foreign intelligence collection operations or other criminal activity.

- When provided to DIB members, US Government indications and warning (I&W) intelligence frequently lacks context, is too heavily focused on domain and IP blacklisting, provides little or no finished analysis, and is generally too old to constitute actionable information.

- US federal law enforcement and counterintelligence agencies need to inform relevant private sector information security staff what is being targeted in cyber operations by our adversaries and, to the extent they know, why to enable predictive analysis necessary to prevent future attacks.

- The US Government, whether DoD or DHS, must provide incentives for the private development of promising technologies that move the community away from outdated signature-based detection modalities and instead focus on powerful combinations of sophisticated behavior analysis and change detection for enhanced anomaly identification.

- The government can identify the best technologies and protocols and then drive government networks towards them.

What can the US Government do to best assist you in improving your cyber security in the long term?

- US Government entities can focus on technologies or strategies that allow DIB members to shift from a passive, forensics-based defense to an active posture incorporating real time intelligence updates that anticipate the adversaries' targets and tactics. Government policymakers must combine innovative technology solutions with substantive diplomatic, economic, and policy efforts abroad to make our adversaries' operational costs and risks unacceptably high.

- The US Government needs to provide greater research incentives for next generation behavior based technologies. If the government invests in game changing technologies and provides incentives for the market to invest in them, DIB members can raise the bar on cyber defense technologies. The current market will partially drive that process, but it is currently confined to creative pockets. Measures to stimulate increased market pressure will drive this innovation into broader market spaces.

- Government agencies can create a regulatory mechanism for information sharing that provides incentives for the DIB members to divulge intrusion information in a safe or non-attributive forum and that ensures good-faith data sharing efforts do not result in lost acquisitions, weakened competitiveness, or similar punitive outcomes from DoD and other government policymakers.

- US Government innovation centers such as DARPA, IARPA, and In-Q-Tel can be leveraged to provide the R&D funds, expertise, and incentives for technology development to make defense industry networks a hard target for the adversary.

- Invest in research in tamper proof protocols. Use these protocols on and between government networks. The commercial world will follow. If government continues to buy Commercial Off-the-Shelf products, though, they will always lag the market instead of driving it.

If you had 5 minutes to discuss cyber security with President Obama what would you tell him?

➢ The US is facing a severe national security challenge from a pervasive, deep penetration of government and private industry information networks by foreign intelligence and organized criminal entities. These efforts have the potential to erode the nation's position as a world leader in S&T innovation and competitiveness. Foreign intelligence services and sophisticated criminal enterprises have discovered that US government and private sector information, once unreachable or requiring years of expensive technological or human asset preparation to obtain, can now be accessed, inventoried, and stolen with comparative ease.

➢ The return on present investment for targeting sensitive US information in this way is extraordinarily high and the barriers to entry extraordinarily low.

➢ Cyber-based operations are the new intelligence battle space of the 21st century and we are currently ill-prepared to defend ourselves. US infrastructure and information networks remain virtually wide open to the sophisticated attacker, be they state sponsored intelligence or purely criminal in mission.

➢ We can't control the Internet, it is woven too deeply into the international fabric and is too unstructured. The entrepreneurial spirit that drives the Internet allows good ideas to bubble up and circulate immediately; however, the same is true for bad ideas. This dynamic creates significant background noise in the world of emerging technology and innovation.

➢ Cyber security is not a problem that we "solve" but rather, like Cold War-era intelligence threats, is a risk to be managed by a combination of generational leaps in defensive technology, paradigmatic shifts in analytic approach combined with strong diplomatic and economic policy initiatives abroad. These efforts, operating in tandem, can ensure that the United States counters this existential threat to our S&T competitiveness while safeguarding long term national security.

Higher Education

What are the greatest problems your company (or industry sector if you prefer) perceives regarding cyber security?

The problem begins with an extreme shortage of highly qualified US graduate students. The educational system must produce more students with strong skills in mathematics and science. Ultimately we need more candidates interested in pursuing masters and graduate degrees in cyber security.

A related problem involves Government regulations which limit foreign students specializing in this area to work in the US on cyber security issues. When foreign students seek admission to pursue cyber security research, they are often denied because NIST sensitive technology restrictions prohibit them. These restrictions further limit the availability of candidates to expand the technological boundaries for improving cyber security.

Incentives must be used to assist both industry and government to adopt rapid deployment of technological innovations of more secure technology into their systems. There are deployable technologies that exist in universities or have been developed by industry, but they are not deployed because the marketplace is unwilling to pay for it. Better biometrics, routers featuring IP trace back and other technological improvements exist but do not get deployed largely due to the economic realities of the global economy.

Eighty-five percent of infrastructure is privately owned, but the owners of these critical infrastructures lack incentive to upgrade to newer more secure systems. In short, there is a tussle between developing and deploying more secure technology and having somebody pay for it.

What are the biggest obstacles you perceive for your University (or industry sector) in addressing the major problems related to cyber security?

The biggest obstacle is the lack of adequate research funding. Available funding is random and inconsistent and lacks structured 6.1 and 6.2 type programs that allow Universities to establish Centers of Excellence which are clearly paramount from an academic perspective.

What can the US Government do to best assist you in improving your cyber security in the short term?

Government must become more industry oriented, focusing not simply on broad national questions but also addressing the questions individual corporate users of technology face.

Security carries hard costs in a marketplace where most users do not recognize it as a feature that provides greater value. The Government must provide adequate and ongoing funding for research and development of better cyber security technologies. If this is a serious national priority it needs to be

treated that way. At the same time, incentives must be creatively employed so industry will be able to justify a business case for investing in more secure technology and systems.

Cyber issues change rapidly so there is a need to continually expand the human supply chain of well trained individuals who will keep us ahead on the technology stage. This is critical not just for security but rather to our Nations economy as a whole. We need to build up a critical mass of people who are expert in this area and will continue to work on these issues here in the United States.

What can the US Government do to best assist you in improving your cyber security in the long term?

Create a system that provides both direct investment, and incentives for private investment in developing research which leads to both human resource development and also the creation of technologies. This in turn will lead directly to new opportunities to create start up companies and to development of new lines for existing companies. This is the formula for fueling our economy in the 21st century.

If you had 5 minutes to discuss cyber security with President Obama what would you tell him?

➢ There is a very strong and urgent need for both industry and higher education to invest in cyber security.

➢ Privacy and security are not opposing forces; we must and can have both. Technologies themselves can be applied to provide the foundation for basing decisions which provide only appropriate and necessary information.

➢ Legislation must be passed in an informed manner and then only to address limited and specific areas if it is to be effective. This requires adequate background knowledge and expertise so policy makers must become more conversant with technological issues that are constantly evolving and have come to dominate our world.

➢ Congress ought to regularly hold hearings and bring in stakeholders to inform our legislators on technological issues. This ongoing process should not focus solely on what is technologically achievable, but also on what impact technology will have on business, people, security, environment, etc. Congress must recognize that technology can not be understood in a vacuum – for example anti-spam legislation without IP trace back can not be enforced. Further, although IP trace back technology exists, it has not been deployed because the decentralized nature of the marketplace has made it impossible to find an appropriate population willing to bear the costs.

Information Technology

What are the greatest problems your company (or industry sector if you prefer) perceives regarding cyber security?

➢ Increasing complexity and power of external threats that have the ability to target infrastructures and unleash an attack with simple tools which are untraceable. We must mitigate the ever-increasing abilities of today's cyber criminals to penetrate the current information security barriers, fire walls, etc. of industry and government organizations in order to gain access to the most sensitive and confidential private information stored in its databases.

➢ Combating the "Insider Threat." To date, most of our efforts have been focused on external threats and not internal ones. We need to reduce the risk of accidental or malicious and criminally-funded access to confidential and private information by inside sources such as employees, consultants or business partners that can be used for extortion or other illegal purposes. The threat posed by someone who has been deemed trustworthy and who has authorized access to critical systems or someone who goes rogue and intentionally or accidentally introduces malware into the systems or does things to the systems or customers in a harmful way without our knowledge is potentially more insidious than the outsider threat. We need to develop a comprehensive and sustainable system to combat both.

➢ Getting the attention of board level management to focus on the risks faced by not having an effective information protection program in place and then convincing them to provide enough financial resources to pay for one.

➢ The holy grail would be to develop a single software or hardware solution that can be effectively deployed across multiple platforms and disparate databases commonly used in most commercial and governmental organizations throughout the world and to implement it as quickly as possible. Until such time as that is practical, a full systems approach to cyber security is necessary.

What are the biggest obstacles you perceive for your company (or industry sector) in addressing the major problems related to cyber security?

The biggest obstacle is that many organizations personnel in both the public and private sector are still not doing enough and are not even sufficiently educated to protect information at rest, in transmission or while being shared.

Awareness must be raised regarding the risks businesses, governments and individuals are taking every day by not taking the appropriate defensive actions. Once this has been addressed, the next steps such as designing the best business processes to employ and selecting the best technical solutions to implement will be easier to accomplish.

However, the very nature of the Internet and related information systems themselves makes the task immensely difficult to resolve with a single magic bullet. The complexity of the technologies being used today coupled with ever evolving threats make the steps needed to confront the threats very difficult to deploy across diverse infrastructures. This reality argues not for a single all encompassing simple solution but a system of integrated and dynamically evolving solutions deployed in a comprehensive and sustainable fashion.

Added to the dual obstacles of a lack of full appreciation of the threat, and the complexity of the systems threatened is the huge distraction of compliance. It is critical to appreciate that there is a difference between regulatory compliance and security.

Currently many businesses spend so much time on compliance measures that may not be related to the major current threat vectors that they fail to address major or even significant threats we need to be focused on.

In a world where the vast majority of the information network is owned and operated by a diverse private sector, security issues cannot be properly addressed with out accounting for their economic impacts. If compliance regimes take money and resources away from real threats, these efforts are not contributing to solving the problem and may actually make things worse.

What can the US Government do to best assist you in improving your cyber security in the short term?

Government needs to share key intelligence and investigation results to give its partners in industry the needed insights that can be used to address the security threats we all face.

Government should create and sponsor programs whereby commercial and government organizations are made aware of the daily risks they are facing and the consequences of not taking the appropriate measures to protect the private information they are shepherding on behalf of their customers and citizens.

Government can embrace the security standards, practices and guidelines that have been shown to be effective in addressing and mitigating known threats.

To assist the private sector, government must provide incentives to organizations that take the steps necessary to effectively protect their data and systems. Numerous programs to provide incentives for industry have been used in various sectors to stimulate private actions that have a public interest benefit. Incentives that have historically been used in other portions of the economy need to be adapted to the cyber security space.

In addition, government must immediately develop a long term strategy to address cyber security and share this with the private sector. It would be helpful not only for the private sector to know where we have to invest now, but also to address future needs that the government is not yet planning to address in a more efficient and systemic manner. Moreover, government can partner with industry much more effectively by engaging with us earlier, on a more equivalent basis to address each other's unique as well as mutual needs.

What can the US Government do to best assist you in improving your cyber security in the long term?

Invest in research. Government funded research has always been the cornerstone of the Internet.

There are aspects to the cyber security problem that simply do not have a business case for addressing. This is the role government must fill and address. This would include protocol research, specific research into products for secure ID management, encryption etc.

One approach might be to develop a modern identity management system to replace the old social security system that was never intended for its current broad usage. The biggest threat to e-commerce is trust since once a nefarious character obtains key information, identities can be stolen or their data can be manipulated. For example, a social security number can be used without you --- not much of a secret --- but it's a meaningful number someone can use for another purpose without your knowledge. We need to develop a way to verify identity while not relying on anything except what is actually relevant to the person. If we could create a system that can't be tied to you except where its totally appropriate, that would be a major step ahead in security These are the kind of things that will provide long term protection against electronic theft while still maintaining privacy and security.

Monitor the results that short term solutions produce and continue to educate both private and public organizations to increase awareness of the negative effects a data breach can cause.

If you had 5 minutes to discuss cyber security with President Obama what would you tell him?

The growing cyber threats are the single biggest thing to affect our economy, and perhaps our physical security long term, yet it is not being properly addressed.

The security of information is a fundamental aspect of modern civilization. Without it, or having it in weakened form, we may suffer irrefutable damage that can be quickly and far too easily inflicted massively on individuals, government institutions and business.

Waiting for others to somehow solve such problems is no longer rational in that the problem worsens by the day. Business and government must act in concert to address this issue quickly and we must do so in a true partnership.

Government must first educate itself regarding the extent and the unique and historic nature of the cyber threat. Then, an extensive awareness program can be launched; however awareness alone will be insufficient.

Information security is a global issue for many of the same reasons as is our economy.

Both from the human perspective and that of technology, the United States can and should be the world leader in this matter. Impressive work, particularly in the area of personal privacy protection, is being accomplished around the world.

The United States has the capacity in resources and talent to focus and develop consensus through international agreements plus have the technology to force information security issues back to manageable form.

In conjunction with government agencies and leading industry consortia, programs can be launched and developed to bring about substantial international improvements in information security worldwide. What is currently missing are United States government programs and necessary industry incentives to raise the required support for the United States of America to seize the opportunity to become the international leader in information security. The Internet Security Alliance stands ready, willing and capable to assist.

What are the greatest problems your company (or industry sector if you prefer) perceives regarding cyber security?

The biggest problem is that, in attempting to ensure security, we are trying to find technological solutions to social problems.

As Bruce Schneier, probably the foremost security expert in the world today said, "Security is never broken, only bypassed".

Most breaches are caused by people behaving poorly in ways that increase vulnerabilities and decrease security. This arises from the fact that people do not have a good "mental model" of what risks are lurking out there.

After decades, or perhaps centuries, of experience, people have pretty much figured out for themselves basic safety rules such as "Don't leave your door unlocked if you are going to be away for a long time," "Don't go out alone at night," Don't go into that part of town after dark," etc.

Similar safety rules for cyber security simply haven't registered with people for the simple reason that they don't perceive any risks, and think of safety rules as burdensome.

Unlike a burglary for example, safety breaches are not immediately visible, nor even immediately damaging. For example, visits to rigged web sites do not always result in instantaneous theft of one's identity. As long as people place convenience above security, we cannot improve the security environment.

What are the biggest obstacles you perceive for your company (or industry sector) in addressing the major problems related to cyber security?

1. Customer reluctance to pay for security
2. Lack of proper incentives
3. Lack of accountability

Security costs money! Not a lot of money, but it does cost some money. Security in general and, cyber security in particular, must be addressed not only as a technological issue, but also as economic and social issues. The lack of understanding of these dynamics is a core obstacle to solving them.

For example, the same people who would happily pay a $25 per day collision damage waiver when they rent a car, knowing full well that the chances of a collision are slight and that the insurance fee is extortionate compared to the actual risk of a collision, would simply balk at a monthly $25 fee to ensure some rudimentary security measures for home PC's.

The anonymity of the Internet provides a venue where many individuals place convenience above security. Most contemporary legal procedures require very elaborate and unambiguous linkage of a cyber identity with a human identity, which is all but impossible in most cases.

Similarly, in an attempt to entice people to upgrade their PCs even when the old ones are perfectly fine, software companies keep on introducing ever more features into the PC's operating system, thus opening many vulnerabilities. This marketing procedure has created an implicit economic incentive to create greater cyber insecurity.

The liability provisions for software vendors are inadequate. Witness for example, the Microsoft EULA, which disclaims all manner of responsibility and liability. If a comparable disclaimer were to be made in any other sector (food, toys, clothing, automobiles etc.) such a product would be banned! But, in software, Microsoft can merrily persist with selling software at risk for breaches with the aid of such disclaimers.

What can the US Government do to best assist you in improving your cyber security in the short term?

The US Government must get its priorities right.

Too often "cyber security" is confused with "anti-piracy." The average Joe or Jane downloading copyrighted content from Youtube is not a cyber security issue, whereas organized gangs systematically collecting and exploiting personal data is a cyber security issue.

One might question if the US government is devoting the proper time and attention to the cyber security issues that are truly most in need of national attention.

The number of such gangs is surprisingly small, but thus far the US Government has not shown sufficient zeal in pursuing such gangs across international borders.

At the same time, the US Government (through CERT for example) has placed very silly barriers when it comes to sharing its vast knowledge of cyber security vulnerabilities and fixes with non-US entities, be they individuals or organizations.

Cyber crime knows no "natural" boundaries. In this domain, the real distinction has to be between people who share our values and those who do not. Entities in countries that share the values of American society must be empowered to ensure their own cyber security through complete and unfettered access to whatever knowledge the US government has in this domain. This is the only way to shore up friendly nations and to isolate rogue nations.

On a related note, the US Government can also insist that every package of software it purchases must come with a sufficient "security rating".

What can the US Government do best to assist you in improving your cyber security in the long term?

The government can foster unfettered sharing of information across international boundaries, and motivate companies to warrant the security of the products they sell.

If you had 5 minutes to discuss cyber security with President Obama what would you tell him?

1. Set clear priorities for our nation's cyber security.

2. Target criminal organizations, not individuals.

3. Expand your cyber security outreach based on cooperative business relationships including those of multi national companies.

4. Modernize your approach to sharing information.

5. Create the right incentives against selling unwarranted software.

Manufacturing

What are the greatest problems manufacturers perceive regarding cyber security?

Our nation's cyber-infrastructure is critical not only to American manufacturing, but to our overall national security. As the U.S economy grows increasingly dependent on the Internet for communication, commerce and homeland security, it is critical that policy-makers make Internet security a continued priority in national homeland security initiatives and preparedness activities. Because private industry owns the networks over which the Internet resides, the Federal government can advance homeland security preparedness through increased collaboration and coordination with the private sector.

Protecting our cyber-infrastructure is of critical importance as Internet-based attacks are on the upswing. In the early days of Internet use, attacks came mostly from cyber-hooligans; now the attacks are more sophisticated and stem from organized crime and hostile nations. A recent study revealed that prime targets of cyber-attacks are small- and medium-sized businesses, with one-third of them having been attacked more than four times in the last three years. The research concluded that a quarter of those attacked (28 percent) took at least a week to recover—a devastating time to be offline for small firms that conduct business and sales via the Web[1].

Regardless of business size, viruses, hacker intrusions, spyware and spam can lead to lost or stolen data, computer downtime, decreased productivity, compliance issues, lost sales and even loss of reputation. A recent survey of 5000 global firms estimated that the direct costs of cyber attacks and consequent lost business can add up to $2 million for each occurrence[2]. In addition, almost a third of the businesses reported computer intrusions to law enforcement[3]. To ensure the security of the U.S. economy, the government must partner with industry – through both open channels of communication and targeted incentives — to bolster key resources and adopt best practices.

What are the biggest obstacles you perceive for manufacturers in addressing the major problems related to cyber security?

Cyber-security is critical for manufacturers of all sizes, but no one-size-fits-all approach can effectively address the problem. Large manufacturers realize the problem, but due to lack of timely information from government resources, quite often remain ignorant to the immediacy of certain threats. Smaller manufacturers understand the necessity of securing their online networks and supply chains, but aren't made sufficiently aware of the urgent priority of taking the next step of securing them. In this situation, education of the domino effect of cyber-threats is needed, as well as information on what constitutes good 'cyber-hygiene'.

Historically, manufacturers look at maintaining their sales, schedules of delivery and the economics surrounding their industries in order to make informed decisions about capital expenditures. Information systems play an important role in their day-to-day business operations, but information security is just as robust as it needs to be to protect their assets. Speculative spending on security for a possible cyber hurricane is an increasingly tough sell, especially in the current economic situation.

The biggest obstacle in addressing this has to do with the flow of information from the government to industry. It is one thing for the government to say industry needs to pay attention to security, but it is quite another for government to identify specific issues and problems, and in a timely fashion. With real-time, specific information industry would appreciate this as a real problem and not a speculative one.

What can the US Government do to best assist you in improving your cyber security in the short term?

In the short term, education and information is needed, as mentioned above. Within every industry, there is one critical factor that separates success from failure. With manufacturers, being able to make their commitments on time is a major concern. The efficient dissemination of information – specifically potential threats to their business operation – is the hallmark of an efficient market. When the government has information that manufacturers need to understand for the security of their business investments, it must be shared in a timely manner.

What can the US Government do best to assist you in improving your cyber security in the long term?

With regards to cyber-security, policy-makers should support polices that:

➢ Allow the private sector to continue developing appropriate general and industry-specific best-practices for improved security;

➢ Give manufacturers of critical technologies with U.S-based manufacturing plants procurement preference for defense and homeland security applications;

➢ Require that any technology solutions be open, interoperable and incorporate industry-based best practices and standards; and

➢ Use identity management solutions and secure communications to limit network access.

More broadly, in order for free-market efficiencies to work, legislators can encourage the private sector to maintain effective Internet security programs and infrastructure by advocating legislation that would:

➢ Allow companies that meet established private sector standards and best practices (as determined by the Department of Homeland Security) to acquire additional cyber security insurance in order to manage losses resulting from catastrophic events;

➢ Establish a national program for temporary, short-term reinsurance to allow insurers to buy reinsurance coverage and provide underwriting assistance for insurance companies;

➢ Limit liability to third parties, exclude liability for consequential and punitive damages and limit liability for non-economic losses; and

➢ Reform privacy rules – including uniform breach notice rules – to limit liability for breaches of companies using standards-based security and best practices.

Also, as the primary innovators in the United States, manufacturers clearly understand that research and development (R&D) drives both new product development and increased productivity, especially in the area of cyber-security. The public sector plays a major role in innovation and represents a key player in the effort to increase federal funding for basic R&D. Over the past 60 years, government-funded research has contributed to major breakthroughs in science and technology. Through the Manhattan Project, we harnessed the atom; through NASA[4], we unleashed space travel; through ARPA [5], we grew the Internet; and through SEMATECH [6], we shrunk the microchip.

Federally-funded R&D is what sets the United States apart from the rest of the world. The $93 billion of federal funds invested in R&D in 2004 [7] exceeded the expenditures of all other G-8 nations combined, with 55 percent of the funding going to universities and federal labs [8].

In order to ensure that ground-breaking achievements continue – especially in the area of cyber-security – it is critical that policy-makers both authorize and appropriate adequate funds for important government research agencies such as the National Science Foundation (NSF), the Department of Energy, the National Institute of Standards and Technology (NIST) and NASA.

Legislators should appropriate increases in research investment authorized by the America COMPETES Act [9] that:

➢ Double funding for the NSF from approximately $5.6 billion in FY'06 to $11.2 billion in FY'11;

➢ Set the Department of Energy's Office of Science on a track to double funding over ten years, increasing from $3.6 billion in FY'06 to over $5.2 billion in FY'11; and

➢ Increase funding for the NIST from approximately $703 million in FY'08 to approximately $937 million in FY'11 and requiring NIST to set aside at least eight percent of its annual funding for high-risk, high-reward innovation acceleration research.

If you had 5 minutes to discuss cyber security with President Obama what would you tell him?

Our nation's cyber-infrastructure is an interconnected combination of private, public and government networks. Manufacturers not only maintain a large portion of that infrastructure, but are an exceptionally important element of our innovation economy. It is critical that government and industry work closely to protect both the infrastructure and the future of innovation.

Giving them the tools to ensure they can protect themselves – access to timely action-oriented information and availability of insurance for cyber incidents – as well as encouraging critical cyber-security R&D here in the U.S., are the most important efforts the new Administration can take to secure our cyber-infrastructure.

1 "Does Size Matter? The Security Challenge of the SMB"; McAfee; July 2008.

2 "Internet Business Disruption – Loss Rates for Global 5000 Firms," Aberdeen Group, June 2004.
3 2007 CSI/FBI Computer Crime and Security Survey.
4 National Aeronautics and Space Administration.
5 Advanced Research Projects Agency was the forerunner of DARPA, the Defense Advanced Research Projects Agency, an agency of the United States Department of Defense responsible for the development of new technology for use by the military.
6 SEMATECH (SEmiconductor MAnufacturing TECHnology) is a non-profit consortium that performs basic research into semiconductor manufacturing, created to solve common manufacturing problems and regain competitiveness for the U.S. semiconductor industry that had been surpassed by Japanese industry in the mid-1980s.
7 Congress of the United States, Congressional Budget Office Report "Federal Support for Research & Development," June 2007.
8 Hon. Richard Russell, Associate Director for Technology, White House Office of Science and Technology Policy; "From the Laboratory to the Living Room: How the Results of Federally Funded R&D are Transferred to the Economy," May 2008.
9 Public Law 110-69.

Detailed Appendix

Introduction

The recent election was clearly a mandate for change. Nowhere is change more critically needed than in our nation's approach to cyber security.

The Internet Security Alliance (ISA) strongly urges the incoming Obama Administration and 111th Congress to consider change in four major areas of cyber security.

First, there must be a substantially increased emphasis on, and investment in, addressing the serious and growing problems our nation, and our allies, face with respect to cyber infrastructure security.

The core protocols upon which the Internet was built are over 30 years old and were not designed with security in mind. Moreover, the explosion in mobile devices, based on the same insecure systems, has dramatically increased the ability to access the system for nefarious reasons. Attacks are on the increase, our defenses are weaker.

Cyber security is no longer the domain of high school hackers but is populated by organized criminals unfriendly nation states and terrorists. The problems we face are far more severe than compromised personal data. Our physical security is threatened by vulnerabilities in our electronic information systems.

Second, the needed investments in this system must be understood for what they really are, critical infrastructure maintenance and security.

It is now a national priority to develop a low carbon, green economy by investing in clean infrastructure which will create jobs and increase our security. Electronic commerce is the ultimate clean technology. However, even universal broadband access, without true cyber security will not achieve this goal.

More than $3 trillion dollars –a quarter of our nation's economic value --moves through the network every day. Virtually every element of our nation's activity, including defense, finance, communications energy, manufacturing, etc. is now reliant on these electronic systems. Low cost investments in securing our electronic infrastructure through both technology and business practice can generate tremendous long and short term gains.

For a century capitol, including foreign capitol flowed into the US because our country was understood to be a safe place to conduct commerce. The growing vulnerability in our cyber systems threatens to undermine that confidence.

Third, the fundamental orientation toward cyber security needs to change. Cyber security is not (solely) an "IT" issue. It is an enterprise wide risk management issue.

Indeed the most common avenue of cyber incursions is through insiders who have the electronic keys to the system. To attempt to address cyber security without appreciating the economic, legal, human

resource, communications, as well as the Information Technology aspects is to fundamentally misunderstand the issue.

Forth, government and industry must develop a much more thoughtful, fundamental and contemporary relationship to address their mutual (not just government's) cyber security needs.

Neither the laissez faire approach of the Bush Administration's National Strategy to Secure Cyber Space nor a system of federally determined mandates are likely to succeed in accomplishing our goals.

Government must embrace some inconvenient truths. First, is the fact that the diversified nature of the internet places many critical national security operations in private industry's hands. This does not mean government has a lesser role, just a different, and frankly 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 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, Washington 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.

Industry and government must construct a mutually beneficial social contract which addresses, creatively and pragmatically, the security of our cyber infrastructure.

The good news is that we actually do know a great deal about how to construct strong cyber systems. Experts and independent research have continually reported that by following identifiable security practices between 80 and 90% of attacks can be thwarted. Our first task needs to be providing the incentives for people to do what we already know can work to substantially curb this massive threat.

With a coherent strategy, we believe substantial progress can be made in addressing the bulk of the problem with appropriate industry incentives. Progress in this area can come fairly quickly. The other 10% of the problem is very sophisticated and aimed at high value targets. This is a very dangerous situation requiring immediate intensive federal attention, and the four conceptual changes cited above.

The Cyber Security Social Contract

A social contract is essentially a deal between industry and government wherein both entities agree to provide and receive benefits resulting in a larger social good.

The cyber security social contract ISA is proposing is based on the agreement between government and utilities in the early 20th century which had the goal of providing universal phone, power and light service to Americans everywhere. That model worked.

In the early 1900s the government realized that there would be enormous public benefits to universal utility service ranging from economic development to enhanced public safety. Policy makers understood that much of the needed infrastructure development would be undertaken thanks to the market incentives inherent in providing these services. However, government also realized that these natural market incentives would not extend to the entirety of the population. Moreover, policy makers realized that it was completely impractical for the government to either fund the infrastructure enhancements needed for universal service themselves or simply mandate that it be done.

In an enlightened and pragmatic move, government struck a deal with the utilities. The utilities guaranteed to make the infrastructure upgrades necessary to provide universal light, power, and telephone service. In return government essentially guaranteed a return on the private investment required economically sufficient to make the investments good business decisions. The utilities maintained the investments over time because they were also provided exclusive franchises for the service area.

In this instance government harnessed the power of private investment to achieve vital social goals, which had the added benefit of stimulating greater economic growth. Meanwhile consumers were protected by the requirement to provide service at government regulated rates. A similar model ought to be developed for cyber security. The necessary infrastructure improvements, technical and otherwise, can be addressed through incentives for private investment while the cyber related consumer protection items (SPAM/personal identity) are addressed by regulation.

While not identical, the parallels between industry and government needs with respect to cyber security are striking. As with public utility service, cyber security cannot be provided directly by the government. As with utility service, many companies do an excellent job with information security as required by their business plans. Also as with public utilities, inherent market incentives are insufficient to provide the breadth of security required by the public's compelling national economic and security interests.

Since a voluntary system will not provide adequate market incentives to accommodate the public interest, and due to the global nature of the Internet, a federally mandated system will not work. A social contract wherein government provides incentives for the private sector to make the cyber security investments that are not justified by current business plans is a pragmatic alternative.

This report outlines what the Internet Security Alliance Board of Directors believe are the most serious problems facing the nation with respect to cyber security; what the government can best do, both long and short term to address these needs and it specifies a series of steps the Obama Administration and 111th Congress can take toward establishing a coherent, pragmatic, effective and sustainable system of cyber security

Why the Internet is Different

For industry and government to create a sustainable and effective system of cyber defense we need a fundamental re-thinking of how we go about addressing these issues.

The Internet is a technology unlike anything we have dealt with before.

> ➢ It transmits phone calls but it is not a phone line.
> ➢ It makes copies but it is not a Xerox machine.
> ➢ It houses books but it is not a library.
> ➢ It broadcasts images but it is not a TV station.
> ➢ It 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" to which we have applied a common noun. The independent networks are knitted together -- some public, some private -- all transmitting information across corporate and national borders without stopping to pay tolls or check regional sensitivities.

One of the most common misconceptions about Internet security is that it is a technical problem. It is not. Cyber security is an enterprise wide risk management problem that cannot, and should not be approached primarily through technological interventions. Indeed the most common path for invasion of information systems is by insiders who have the technological keys to entry.

Unlike traditional infrastructures, the mode of Internet attack changes constantly over time. The vast, largely benign worms and viruses of past years have long given way to phishing attacks which in turn have been replaced by individualize "designer malware." Indeed even the very notion of time itself is different with respect to the Internet. Often attacks are "launched" and lie dormant for extended periods only to be "executed" at an entirely different point in time.

To address Internet security as a technical issue without simultaneously addressing the economic, human resource and other risk management issues is to fundamentally misunderstand the issue.

Why the National Strategy is Not Working

In 2002 the Bush Administration released its National Strategy to Secure Cyber Space. ISA supported the philosophy of a market based, as opposed to regulatory mandated approach. However, ISA has always maintained that the "missing link" in the National Strategy is the lack of an incentive program to bridge the gap between the security investments that industry would make for their own corporate needs, and the additional investments that may be required to accommodate the broader national interest.

The National Infrastructure Protection Plan the Bush Administration published in 2006 essentially acknowledged that this gap exists, however no serious attempt to construct the needed incentives for additional private investment in cyber security have been made.

It is now apparent that the approach in the National Strategy has not worked. Research has consistently indicated that we are simply not reaching enough corporate leaders.

Among the alarming findings of recent studies are:

- ➢ 29% of senior executives acknowledged that they did not know how many negative security events they had in the past year.
- ➢ 50% of senior executives said they did not know how much money was lost due to attacks
- ➢ 23% of CTO's did not know if cyber losses were covered by insurance.
- ➢ 34% of CTO's thought cyber losses would be covered --- and were wrong.

Most recently CIO Magazine in conjunction with PricewatershouseCoopers surveyed more than 7,000 business and technology executives and published the results October 15 2008.

Among their findings:

- ➢ Only 59% of respondents attest to even having an overall security policy
- ➢ Nearly half of all respondents said they can't identify the source of information security incidents they have suffered in the past year
- ➢ Employees and former employees are the biggest source of security incidents accounting for half of the ones we can trace
- ➢ Only about half of respondents provide employees with security awareness training
- ➢ Only 56% of respondents employ a security executive at the C-level --- down 4% from the previous survey
- ➢ Only 43% audit or monitor compliance with security policies (if they have them)
- ➢ Just over half of companies (55%) use encryption
- ➢ 1/3 of respondents don't even use firewalls
- ➢ Only 22% of companies keep an inventory of all outside parties that use their data

In short 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.

Why A Regulatory Model Won't Work

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 revolutionary Internet system effectively.

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 investment and federal regulations have little track record for stimulating sustained investment. In a global economy industry can easily move production off shore which creates additional economic and security problems for the US.

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 two centuries ago --- the railroad.

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
- A US law could put US industry at a competitive disadvantage at a time we can least afford it
- Even if an 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
- A federally specified metric of information security to be applied to the vast private sector would not appreciate the various sector specific differences which must be considered
- Such an approach would be too static
- Might be weaker than needed due to constant political pressure
- Could even be counter productive to constantly enhanced security needs of ever evolving technology
- It would also be extremely difficult to enact legislatively wasting valuable time

The Good News - We Do Know What Works

The good and underreported news is that we actually do know a great deal about how to secure our information systems ---- the bad news is that not enough organizations are doing it.

However the first goal of the Obama Administration and 111th Congress ought to be identifying the practices and policies that have been shown to work and providing practical motivations to encourage their widespread adoption.

Within the marketplace there is a robust assortment of published regulations, standards, best practices and similar guidance's that have already been produced to address 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 compliance with these existing practices can indeed result in demonstrable improvements in cyber security.

One of the largest security research projects ever done, the 2004 "Global Information Security Survey" conducted by PricewaterhouseCoopers, found adherence to industry developed best practices provides a substantial positive effect on overall cyber security. The study identified about one-fifth of their respondents, dubbed the "best practices" group. These respondents reported 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 "best practices" group reported that they 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 breech Investigations Report" conducted by Verizon. This study drew on over 500 forensic investigations over a four year period including literally tens of thousands of data points. It concluded that "Perhaps the most significant statistic coming out of this historical analysis is that in 87% of cases investigators concluded that the breach could have been avoided if reasonable security controls had been in place at the time of the incident".

Robert Bigman, of the CIA provided further corroboration while speaking at an Aerospace Industry Association meeting regarding the breaches being experienced by the government. "Contrary to

popular belief" Bigman said, "actually many of the attacks were not all that sophisticated". He estimated that with simple the use of "due diligence" you could reject between 80 and 90% of attacks. "The real problem is implementation", said Bigman. "You need to find and train good security people."

Core Components of the Cyber Security Social Contract

This report provides numerous specific examples of components that maybe included in the government industry program we are referring to here as the *cyber security social contract*. Naturally with the diversity of the private sector there will never be a single document that comprises the varying relationships. However the contract, as a conceptual framework, would include the following five core elements:

1. Identifying Government's Role

Policy makers must first educate themselves better with respect to the Internet and its role in modern American society. Too many policy makers (and too many of their industry colleagues) choose to defer learning about modern networks, trusting that "the computer geeks" will solve the problems. The Internet has been called the most transformative human invention since the printing press. No one is saying that Congressmen need to personally reconfigure their computers, but to fail to understand the core functions electronic information systems play in our national life ill prepares them to deal with the many policy issues that rely on the sound functioning of the network.

A. **Government must get its own house in order**. Happily government goes through its FISMA program annual audit of its cyber security. Unhappily the scores are often abysmally low. It is obviously inappropriate for government to assert the status to tell industry how it must upgrade its cyber security until the government systems, many of which are not on par with private sector systems, are able to meet their own self-set standards. A substantial government improvement program for all their cyber systems could provide a compelling model for the underachieving portions of industry and provide a platform to drive positive economics for improvements in non-government systems.

B. **Policy makers must establish a program to educate others**. We are not talking just about "awareness" programs which too often have translated into setting up web sites where reams of government data are dumped and the box saying "inform industry" is checked. Such programs are the rough equivalent of sitting first graders in front of computers and telling them to "go learn." We are advocating a thoughtful, funded, aggressive education/marketing program targeted at senior corporate executives such as CEOs, CFOs and business unit chiefs. As with any professional marketing program it must begin not with government deciding what message it wants to send, but with research on the target audience revealing what they need to know. The education must include not just the national interest arguments, but solid business/economic arguments backed by verifiable data.

C. **Government must create incentives for industry to invest in cyber security beyond what is necessitated already by industry's business plans**. If there were a comprehensive ROI for cyber security spending across the totality of the private sector we would not have the problems

and statistics cited earlier in this report. We are now past the time when government can hope that industry will simply fulfill the role of fully funding cyber infrastructure security. Where a return on investment is not justified, government needs to assist in managing the market in the national security interest.

2.   **Identifying Industry's Role**

    A. **Industry must continue to develop verifiable standards and practices that will continually Strengthen Cyber Security**. We suggest encouraging the mechanisms existing within the market to continue to evolve appropriate information security practices, motivated by the development of additional Federal incentives and benefits.

    B. **Implement best practices and standards**. ISA is arguing for the federal government to provide incentives for increased industry security action, but it will remain industry's responsibility to practice the needed due diligence to operate in an increasingly secure fashion.

    C. **Use their businesses to expand the perimeter of security through contracts**. One of the fastest growing areas of vulnerability, even for organizations that do a good job managing their own electronic data, is the shared data with other entities', some of which may be off shore. Industry must work assiduously to develop and enforce contracts and monitoring systems to expand the use of cyber security to partners, clients, customers and agents of their business.

3.   **Identifying What Behaviors/Practices etc. Are to Be Motivated**

There are effective best information security practices already operating in the corporate world; there is a general consensus, however, that no one standard or guidance "fits" all information security requirements for all industries. What qualifies for a specific company or entity as an appropriate best practice will be affected by the size of the organization, the culture – or cultures – within which it conducts business, its sector-specific regulatory status, and a range of other variables.

However, in order to provide the stability and predictability that ISA agrees must be present, the Federal incentives must be associated with those standards that are widely recognized and have broad endorsement. This helps assure there is no effort to merely craft a "lowest common denominator." Specifically, we propose that companies should have available Federal incentives if they implement information security pursuant to, and meeting:

    ➢ **Information security procedures adopted pursuant to, and in compliance with, Federal regulations applicable to the industry in which a commercial entity conducts business**. (This has the effect of avoiding any duplication of rules to which a commercial entity is already subject, for example with respect to personal information.)

    ➢ **Information security standards that are established and maintained pursuant to requirements of "self-regulatory organizations"**. Self-regulatory organizations could be designated for that purpose by appropriate Federal agencies having direct interaction with specific industries, such as financial services.

> **Information security procedures that are established and maintained pursuant to applicable standards published by recognized standards organizations**. Specific sponsoring organizations which could be recognized by the enabling legislation would be:
> 1. International Organization for Standardization.
> 2. American National Standards Institute.
> 3. National Institute of Standards and Technology.

4.   Identifying What Incentives Government will Provide to Industry

There is an extensive history, beyond the utility social contract discussed above, wherein government has used a wide range of incentives to promote social goals which were impractical for direct government provision. Industry sectors as diverse as agriculture, ground transport and aviation, energy, environment, and even security all have been subject to various incentive programs. Policy makers can adapt many of these models to the cyber security issue we address today.

Generically ISA has traditionally suggested policy makers consider the following options:

A. **Congress can use its market power**, instead of its regulatory power by including security more prominently, along with cost into its procurement process
B. **Congress can lead by example** by fully funding federal agency needs for cyber security and integrating security compliance into personnel evaluations along with other HR criteria
C. **Congress can tie incentives such as civil liability safe harbors** (like those provided in the SAFETY Act), or provide procurement credits to companies able to demonstrate compliance with market generated best practices for cyber security
D. **Congress can stimulate the stunted cyber insurance market**. The cyber insurance market has been hampered by a variety of factors including the risk of a massive cyber-hurricane. Government has experience assisting immature insurance markets to grow to stability and then using this tool to generate pro-social goals such as greater adherence to best practices and standards, privately funded auditing of systems and transferring risk from both private and government in the case of a major incident. These steps ought to be adapted to the cyber security arena.
E. **Congress can create an industry/government/university consortium to stimulate the needed research, development and adoption of security protocols**. This would be similar to the Sema-Tech model used in the late 1980s to address the computer chip gap. The analogy in this instance is that industry government and business need to be able to work on issues of broad public policy benefit without market encumbrances at least in areas wherein there is unlikely to be a private market developed. An example would be the development and implementation of new, modern, secure core protocols for the Internet.
F. **Government can create awards programs similar to the "Baldrige Awards"** for quality, which eventually became a sought after market differentiator for corporations. By assisting in providing a market advantage for good security in part by popularizing it, government can assist corporations to invest their own assets.
G. **Government can provide Stafford Act assistance for good actors**. In times of crisis there is often a need for private industry to access additional resources, which is currently impeded by the Stafford Act. Some relief may be found for this by providing an incentive for the

corporations doing the most to assist in pro-social concerns like cyber security if they see an advantage in their own times of trouble.

H. **Government can use the SBA loan system** in a manner similar to what we are advocating for the larger government procurement process. SBA loans could be leveraged as a way to provide greater reach for good security investments and practices among the millions of smaller companies who might not otherwise include such spending in their business plans.

I. **Government can realistically address the legal and corporate issues which are part of the inadequate information sharing system between industry and government**. Moreover, Government can engage in more intensive education programs ranging beyond DC based working groups, massive data dumps on web sites and isolated events. A true, sustained education, as opposed to an "awareness" program is needed.

WHAT IS THE INTERNET SECURITY ALLIANCE?

Virtually every corporation has by now integrated the positive aspects of the digital age into their business plan. However, the negative aspects of the informational age including the threats to corporate intellectual property, business operations and overall security have been less appreciated.

The Internet Security Alliance (ISAlliance) is a non-traditional trade association that is designed as a means to understand, integrate and help manage the multi-dimensional and international issues that operating in the Internet age creates.

WHAT DOES THE INTERNET SECURITY ALLIANCE DO?

ISAlliance provides tangible benefits to its membership by creating cutting edge services and applicable across the various industry sectors that use the Internet.

ISAlliance was conceived in conjunction with Carnegie Mellon University to integrate emerging technological issues with the membership's pragmatic business concerns and align public policy to facilitate business growth and resilience.

The ISAlliance provides a broad range of ongoing technological, business and policy services to its membership which can be reviewed at the web site www.isalliance.org

In addition, the ISAlliance Board identifies a select set of priority projects each year for intensive work. In 2008 the ISAlliance has identified the following priority projects:

- The President's National Cyber Initiative (Bush Administration)
- Cyber Policy Development for the Obama Administration and 111th Congress
- Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask
- Developing Automated Security & Assurance for the VoIP Platform
- Securing the Supply Chain in the Age of Globalization
- Applying SAFETY Act incentives to cyber security

ISAlliance

2500 Wilson Boulevard, Suite 245

Arlington, VA 22201

www.isalliance.org

info@isalliance.org