Testimony of
Larry Clinton, President & CEO
Internet Security Alliance

before the
Subcommittee on Communications and Technology
Committee on Energy and Commerce
U.S. House of Representatives

Hearing Entitled
"Cybersecurity: Threats to Communications Networks and Private-Sector Responses."
February 8, 2012

Executive Summary (oral statement)

There has been a dramatic change in the cyber threat picture in the last 18-24 months.

Our main concerns are not "hackers" or kids in basements. The fact that a cyber system has been "breached" is no longer the metric that determines a successful cyber attack.

Cyber attackers have grown increasingly sophisticated. While so called "hackers" are still a concern, the far greater urgency is to address the ultra-sophisticated attackers of today sometimes referred to as the APT or "Advanced Persistent Threat".

The APT attackers are pros. They are highly organized, well-funded, expert attackers who use coordinated sets of attacking methods both technical and personal. The investment required to carry out these attacks suggests they are often nation-state supported.

Perhaps most indicative of these attacks, if they target a system they will invariably compromise, or "breach" it.

We have seen these attacks for several years in the defense sector however they have recently migrated far more broadly. The most recent research shows that responding to APT style attacks has become the major focus in industries as diverse Utilities, Consumer Products, Financial services industrial and manufacturing sector and even entertainment and media

Unfortunately conventional information security defenses don't work vs. APT. The attackers successfully evade all anti-virus network intrusion and other best practices, remaining inside the targets network while the target believes they have been eradicated."

This doesn't mean we have no defense. It does mean we need to modernize our notion of what constitutes cyber defense. Traditional approaches, including federal regulation will not solve this problem and bad regulation could be counter productive.

Fundamental to stopping the advanced cyber threat is to understand that our biggest problems are not technological, but economic.

Research from Pricewaterhouse, CIO Magazine, CSIS & McAfee as well as ISA's own work has consistently shown that the single biggest problem in combating cyber threat is not technical, it is cost.

Just last week Bloomberg released an extensive study that found to reach an acceptable, not the ideal, level of security in critical infrastructure would require a 91 percent annual spending increase.

The private sector has been extremely responsive to combating the cyber threat. President Obama Cyber Space Review found that "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity"

Our companies are focused on providing a robust, multi-layered defense including extensive automated and business process controls with emphasis on deploying new analytical technologies that help us better understand threat indicators both on the inside of our network as well as our perimeter. We understand that basic security practices are necessary but not sufficient for today's threats so we continue to explore new technologies to help identify and mitigate the Advanced Persistent Threat problem while investing in our workforce. We have developed strong relationships within our sector and outside our sector to share information that leads to a more complete threat picture. We aggressively seek out best practices and share our own.

Despite the fact that our critical infrastructure is under constant cyber attack we have never had an instance of serious breakdown similar to what we have seen for example in the environmental arena.

This success is due in large part to the flexibility generated in the current system which relies on voluntary partnerships wherein industry, which understands and can manage these systems best, can use their intimate knowledge to respond to rapidly emerging cyber threats in a fashion they believe can best protect the system rather than being driven by a pre-set government requirement

Nevertheless there is a great deal Congress, and the Commerce Committee, can do to assist to enhance our cyber security.

1. Get their own house in order

In addition to well know deficiencies from the Weikileeks compromise to poor FISMA scores the National Academy of Sciences the GAO and just last week the DOE Inspector general have all documented systematic problems managing government cyber space. One immediate place to start is the consensus legislative FISMA reforms, which have been delayed for several years

2. Provide the right mix of regulation and incentives

The evidence is overwhelming that the largest barrier to securing cyber space is economic. For industries where the economics of the industry are tied directly to a regulatory format, such as electric utilities, water, transportation etc the current regulatory structure can be used to motivate and fund needed cyber advancements.

For industries where the economics are not inherent to a regulatory structure we need to motivate by providing appropriate market incentives to spur greater security investment. An excellent example of this approach is the Rogers bill passed by the Intelligence Committee with broad bi-partisan support, which uses liability reforms to stimulate additional information sharing.

However liability reform is one of many incentives that need to be unleashed to help secure our cyber networks such as:

- Greater use of government procurement
- Streamlined regulation in return for demonstrated security improvements
- Greater use of private insurance
- Streamlined permitting & licensing
- Stafford Act access

Incentive such as these can be used to stimulate investment, innovation and the adoption of security procedures beyond what is commercially viable.

This approach was advocated by the ISA in the Cyber Security Social Contract in 2008, President Obama's Cyber Space Policy Review in 2009, the Multi-trade association/civil liberties white paper on cyber security in 2010 and the House Task Force Report on cyber security in 2011.

A great deal of work needs to be done to fill out how these incentive models can be best deployed in the various sectors so that needed legislative changes can be made.

In the meantime Congress ought to enact the FISMA reforms and information sharing bills I alluded to above and also strengthen our law enforcement criminal effort and improve the management of federal systems.

Passing this package of cyber reforms would be an historic---and politically achievable accomplishment.

Ladies and Gentlemen of the Commerce Committee…. what you are dealing with here is the invention of gun powder…. mandating thicker armor won't work just like building broader moats wouldn't stop invaders who had invented catapults & just like the Maginot line was no defense against the invading Germans in WWII.

Trying to use 19th & 20th century models & federally regulating the Internet will not be effective. We need a much more contemporary and creative approach wherein the private sector is engaged, not controlled by our government partners. We look forward to working together.

Written Statement of the Internet Security Alliance:

THE EVOLUTION OF THE CYBER THREAT AND THE NEED TO EVOLVE OUR UNDERSTANDING OF IT

THE EVOLVING CYBER THREAT

There has been a dramatic change in the cyber threat picture in the last 18-24 months.

Our main concerns are not "hackers" or kids in basements. The fact that a cyber system has been "breached" is no longer the metric that determines a successful cyber attack.

Cyber attackers have grown increasingly sophisticated. While so called "hackers" are still a concern, from a public policy point of view, the far greater urgency is to address the ultra-sophisticated attackers of today sometimes referred to as the APT or "Advanced persistent Threat."

The APT attackers are pros. They are highly organized, well-funded, expert attackers who use coordinated sets of attacking methods both technical and personal. The investment required to carry out these attacks suggests they are often nation-state supported.

Perhaps most indicative of these attacks, is that if they target a system, they will invariably compromise, or "breach" it.

We have seen these attacks for several years in the defense sector, although they have recently mitigated far more broadly. The most recent research shows that responding to APT style attacks has become the major focus in industries as diverse utilities, consumer products, financial services, the industrial and manufacturing sector and even entertainment and media.

The most common current cyber threat uses a mixture of technology abuse (hacking), white collar (organized) crime techniques, and advertising expertise (phishing, spamming, social engineering, etc.) With that mixture, criminal groups easily manipulate both human and machine weaknesses to gain access to items of value. Those items certainly include money and financial instruments, but also include intellectual property that can be sold. In fact, the entire motivation behind the APT-types of breaches is to steal information, not to cause disruptions. Current proposed cyber legislation is too focused on preventing terrorist-style disruptive attacks and not on preventing online criminal behavior.

While there is increased attention being paid to these ultra-sophisticated threats, traditional defenses are having a very difficult time keeping up with the evolving threat.

Companies are countering the APT principally through virus protection (51%) and either intrusion detection or prevention solutions (27%).

However, “Conventional information security defenses don’t work vs. APT. The attackers successfully evade all anti-virus network intrusion and other best practices, remaining inside the targets network while the target believes they have been eradicated.”

This doesn’t mean we have no defense. It does mean we need to modernize our notion of what constitutes cyber defense.

ECONOMICS: THE MAJOR OBSTACLE TO PROVIDING CYBER SECURITY

Fundamental to stopping the advanced cyber threat is understanding that our biggest problems are not technological, but economic.

It is short sighted to think of the cyber threat as simply a technological issue that can be solved through standards and performance requirements. In reality the cyber threat is much more complex with as many strategic, human and economic issues as operational and technical ones---yet many of the current government actions and new proposals focus almost entirely on operational and technical issues when the real issue is economic.

Independent research has continually born out the fact that security flaws stem as much from poor incentives as they do from bad technological design. In cyber security the current economic incentives all favor the attackers. Attacks are cheap & profitable while defense is expensive, difficult to justify with economic ROI and criminal prosecution is almost non-existent---less than 1%.

Research from Pricewaterhouse, CIO Magazine, CSIS & McAfee as well as ISA’s own work has consistently shown that the single biggest problem in combating cyber threat is not technical, but is cost. Several of these studies also document that although the threat is increasing, spending on cyber

security has been reduced between 50%-66% of American companies over the past few years.

Just last week, Bloomberg released an extensive study that found to reach an acceptable, not the ideal, level of security in critical infrastructure would require a 91 percent annual spending increase.

"In general, organizations recognize that they are very, very vulnerable, and they don't actually have enough resources to get the job done properly," said Larry Ponemon, who conducted the study for Bloomberg.

WHAT IS THE PRIVATE SECTOR DOING?

The private sector has been extremely responsive to combating the cyber threat on several different levels.

The Market has Developed Effective Cyber Security Programs

The private sector has been aggressive in continually innovating and creating standards practices and technologies to counter the cyber threat.

For more than a decade, the ISA and its member companies have been engaged in thought leadership and creating and operating programs designed to enhance our nation's cyber security. Among the programs the ISA has initiated and operated in conjunction with our partners are programs on Enterprise Risk Management, Information Sharing, Insider Threats, Mobile Security, Senior Management Education, Supply Chain Management, Small Business and Home User Security and best practices to help combat the Advanced Persistent Threat.

Although the ISA opens its programs and projects to government participants, it receives no government funding. All ISA programs are supported by voluntary contributions from the private sector. All ISA products and services are available on an open source model and free of charge to all consumers.

The ISA and its members compromise only a small fraction of the investment made by the private sector to secure our overall system. Moreover, industry, and governmental analysis has demonstrated that, if these systems were implemented they would yield substantial success.

Verizon in conjunction with the US Secrete Service has done a series of studies in which they performed a forensic analysis of hundreds of successful cyber breaches, analyzing tens of thousands of data points. The research has documented that had the organizations who suffered the breaches followed standards and practices already existing in the market, they would have prevented or mitigated mitigate the effects of between 95-97% of cyber attacks.

Shortly after taking office, President Obama commissioned the National Security Council staff to review our nation's effort in cyber defense. Their report, "The Cyber Space Policy Review" found that "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity."

Although it is well known that neither the public nor private sectors have been successful in stopping all cyber attacks, we have been successful in preventing our critical enrapture systems from being seriously compromised.

For example, several of the major bills being considered in Congress, including that approved in the House Cyber Subcommittee of HLS and the circulating Senate drafts address cyber attacks of high national significance, i.e., ones that would result in "interruption of life sustaining services sufficient to cause, mass casualty … mass evacuations … catastrophic economic damage or severe degradation of our national security." No less an authority than Homeland Security Secretary Napolitano has asserted that our critical infrastructure is under cyber attack thousands of times a day, which translates into hundreds of thousands of times a year and millions of attacks in just the past few years.

Despite this environment of constant cyber attack, however, there has never been a single instance of cyber attack even approaching the level the bill's draft addresses. This success in protecting our critical infrastructure, while not perfect, is due in large part to the flexibility generated in the current system which relies on voluntary partnerships within industry, which understand and can manage these systems best. These partnerships can use their intimate knowledge plus information provided, at times by the government, to respond to rapidly emerging cyber threats in a fashion they believe can best protect the system.

Federal Mandates Could Compromise Cyber Security

This ability to be responsive to the situation on the ground, without having to worry about complying with a pre-set federal requirement is especially critical in the cyber security space wherein infrastructure owners and operators need to be responsive to novel situations which evolve constantly. In such instances, it is critical that owners and operators dealing with a major attack are focused first and foremost on what needs to be done to mitigate the attack, and not the reading of a pre-set performance requirement.

For example, it might be assumed that performance requirements would be set at such a level of generality that they will not impede the managing of an attack. However, even steps that were a few years ago obvious, such as securing the perimeter or stopping the attack as soon as possible, have now been shown to be either impractical (as in the case of the former) or unwise (as often in the case of the latter). In this rapidly changing environment, incentives to undertake the most effective measures, rather than requirements to follow the government mandate are what we need to be creating to secure our cyber systems.

Moreover, one of the characteristics of the APT is that attackers will virtually always succeed in successfully breaching the targeted cyber system. As a result, a "performance requirement," such as maintaining a breach proof environment may be, in the current context, hopelessly unrealistic and investment toward that end may well be an inappropriate use of scarce cyber security resources.

Most entities are unable to tell whether they have been the victim of a successful sophisticated cyber attack unless they make a special effort to investigate, spend additional resources on the effort, and have the necessary skills and tools already on hand. The initial signs that need to be pursued in order to discover a skilled cyber attack are hard to define, constantly changing, and often very subtle and thus unsuitable for federally derived, pre-determined requirements and the annual evaluation procedure it proposes to rely on. Uncovering a highly skilled cyber attack is currently much more of an art than a science. It can require intuition, creativity, and a very high degree of motivation.

The kinds of language and administrative formulas that would have to be adopted to comply with the proposed requirements would almost certainly have little to do with real cyber security. This is partly because the field is developing so rapidly that by the time cyber security "requirement" were recognized as fulfilling administrative expectations, it would already be obsolete. There is also no way to tell at the level of a "general requirement" whether the cyber security measures involved would be doing any good or not.

The resources required to address the types of attacks we are concerned with here need to be, as they currently and successfully are, based on the experts analysis on the ground, not a federally predetermined standard or requirement.

Major Enterprises are Aggressively Pursuing Cyber Security

Finally, at a enterprise level we are focused on ensuring a robust, multi-layered defense including extensive automated and business process controls with emphasis on deploying new analytical technologies that help us better understand threat indicators both on the inside of our network as well as our perimeter. We understand that basic security practices are necessary but not sufficient for today's threats so we continue to explore new technologies to help identify and mitigate the Advanced Persistent Threat problem while investing in our workforce. We have developed strong relationships within our sector and outside our sector to share information that leads to a more complete threat picture. We aggressively seek out best practices and share our own.

Maintaining the current rate of success in stopping catastrophic cyber attacks, and expanding this success to other sectors will require us to directly address how we finance solutions. The notion that a large complex and serious problem can be easily and cheaply solved with a new government mandate defies common sense.

WHAT SHOULD THE GOVERNMENT BE DOING

Notwithstanding that there is already excellent work being done to secure cyber systems, ISA believes, and has believed since its inception in 2000, that the federal government can and should be doing more to assist in our

cyber defense. Specifically, the federal government needs to get its own house in order, provide the right mix of incentives and regulations to the private sector and, above all, do no harm.

3. Get their own house in order

Congress' role in cyber security needs to centered on leadership rather than law-making. Via Congress' oversight and appropriations responsibilities, the federal government's own networks should be built and operated to world-class standards in terms of security and should set the example for others to match. By setting the bar high for government networks and encouraging state and local governments to follow, industry will find it easier to purchase and install solutions that are already proven to work on government networks. This has the dual advantage of driving new jobs in the technology sector via increased federal spending on cyber security product development and acquisition; and it will push security technology innovation into new areas that might not be reached if left to traditional market forces.

Unfortunately, government has not matured its own cyber processes sufficient to be placed in the position of judging industry's management of the far more diverse systems in the private sector.

For example, the damaging Wiki leaks compromise last year was not a sophisticated attack but the result of rudimentary organizational mismanagement. Moreover the governments own low FISMA scores attest to the need for the government to improve its own management systems and there are numerous other recent examples of the need to mature the federal management systems including:

National Academy of Sciences review of DHS cyber consequences found that they were missing critical elements:

"DHS analyses of consequences have tended to focus on the outcomes that are most readily quantified. Little attention has been paid to secondary economic effects or to an attack's effects on personal and group behaviors—impacts that could be significant and may be the primary goals of terrorists. Some relevant research is being conducted in DHS…but much more is needed. In addition, efforts must be made to incorporate the results of such research into DHS risk analyses and to heighten risk analysts' awareness of the importance of social and economic impacts."

With respect to DHS risk management capability the national Academy found "it is very difficult to know precisely how DHS risk analyses are being done and whether their results are reliable and useful in guiding decisions."As recently as December 9, 2011 the GAO criticized DHS and

other federal agencies for its failures to adequately promote **effective** cyber security measures in its report, entitled "Critical Infrastructure Protection: Cyber Security Guidance Is Available, but More Can Be Done to Promote Its Use," GAO found that:

> "Implementation of cyber security guidance can occur through a variety of mechanisms, including enforcement of regulations and voluntarily in response to business incentives; however, sector-specific agencies could take additional steps to promote the most applicable and effective guidance throughout the sectors . . . Federal policy establishes the dissemination and promotion of cyber security-related standards and guidance as a goal to enhancing the security of our nation's cyber-reliant critical infrastructure. DHS and the other lead agencies for the sectors selected for review have disseminated and promoted cyber security guidance among and within sectors. However, DHS and the other sector-specific agencies have not identified the key cyber security guidance applicable to or widely used in each of their respective critical infrastructure sectors. In addition, most of the sector-specific critical infrastructure protection plans for the sectors reviewed do not identify key guidance and standards for cyber security because doing so was not specifically suggested by DHS guidance. Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Improved knowledge of the guidance that is available could help both federal and private sector decision makers better coordinate their efforts to protect critical cyber-reliant assets...GAO is recommending that the Department of Homeland Security (DHS), in collaboration with public and private sector partners, determine whether it is appropriate to have cyber security guidance listed in sector plans. DHS concurred with GAO's recommendation."

Just last week it was reported that the Department of Energy's Inspector General had found that the Department's rush to award stimulus grants for projects under the next generation of the power grid, known as the Smart Grid, resulted in some firms receiving funds without submitting complete plans for how to safeguard the grid from cyber attacks, according to an

inspector general's report.

"Officials approved cyber security plans for Smart Grid projects even though some of the plans contained shortcomings that could result in poorly implemented controls," states the report. "We also found that the Department was so focused on quickly disbursing Recovery Act funds that it had not ensured personnel received adequate grants management training."

According to the **report**, 36 percent of the grant applications submitted were lacking one or more elements in their cyber security plans. Three out of the five cyber security plans reviewed by the IG were incomplete, and often didn't address weaknesses previously identified by the Energy Department.

It would seem obvious that before Congress granted extended power to the government to make cyber security decisions for the private sector it ought at least to demonstrate they can manage this task for their own, comparatively limited, systems

4. Provide the proper mix between incentives regulation and incentives

It’s obvious neither government nor industry can alone address the growing cyber security issues.

In 2008, ISA proposed an alternative model, a cyber security social contract wherein government would provide market incentives to cover the investments required for industry to take on additional cyber security defense.

In 2009, when President Obama released the Cyber space Policy Review based on a in-depth study by the National Security Council staff the Executive Summary both began and ended by citing the ISA Social Contract The President’s document which specifically urged the consideration of several such market incentives.

In 2010, a coalition of 5 industry and civil liberties groups adopted a similar set of recommendations.

In 2011, the House Republican Task Force adopted as its very first recommendation that congress needs to develop a menu of market incentives to address our collective cyber security problems.

In 2012, we hope to see legislation, such as Congressman Roger's bill, which uses liability protections as an incentive to spur greater information sharing to reach the House floor.

The Rogers bill does more than simply providing a tangible incentive to share information, it signals a more progressive approach to the government industry relationship which moves in the direction that will generate increased cooperation.

Classification, breach disclosure laws, SEC regulations and the like all have their place, but they also have the unintended consequence of inhibiting sharing because they create an atmosphere wherein having information to share is presumed to be indicative of a breach that must be disclosed. What it should be is a celebration that someone has valuable information to share without any question as to how they found it. It is reflected in government language of wanting companies to report compromises when they should be asking industry to report indicators. It is a subtle difference but the former is seen as a confession that risks punishment (official or in the press) while the later is seen as a measure of the skill of the reporting company

The private sector takes cyber security very seriously and is spending a good percentage of their IT budgets on protecting their networks and digital property from relentless criminal attacks. However, the private sector is held back by old laws that discourage the rapid sharing of timely information, and by a general reluctance of local law enforcement organizations to provide the training and advice on how to be secure in cyberspace the same way that information is readily made available for physical security. The private sector needs help, but they don't need additional regulation. Remove the old barriers to rapid information sharing and beef up the capabilities of local law enforcement organizations to "take a byte out of crime" in the digital world.

However, there is a great deal more that needs to be done In addition, to liability incentives there are wide ranges of additional incentives that are low cost to the government but could create powerful incentives to promote additional critical infrastructure security on a sustainable basis. These incentives include:

- Greater use of government procurement
- Streamlined regulation in return for demonstrated security improvements
- Greater use of private insurance
- Streamlined permitting & licensing
- Stafford Act access

This approach is also consistent with the Administration's policy for establishing regulations as articulated in Executive Order 13563, January 2011, which directs agencies to "identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public."

5. Do no harm

ISA has been lobbying for greater government attention to our cyber security problems for over a decade and so we are naturally grateful to see legislation moving to address this problem.

However, there is a difference between realizing that there is a significant problem and developing an effective and comprehensive solution.

Some, surely well intentioned, proposals, not only bear little hope of addressing the issue but run the risk of making things much worse.

No less an authority than the current Deputy Undersecretary for Cyber Security at DHS, Mark Weatherford, has noted the potential danger of moving in this direction:

"As I study [recent] pieces of [cyber security] legislation, the one thing that concerns me is the potential negative implications and unintended consequences of creating more security compliance requirements. Regulation and the consequent compliance requirements could boost costs and misallocate resources — without necessarily increasing security due to placing too much emphasis on the wrong things. It is therefore critical that any legislation avoids diverting resources from accomplishing real security by driving it further down the chief security officer's (CSO's) stack of priorities."

The notion that all we need is a set of federal regulations is vastly over simplified----and potentially dangerous.

Blaming the victims of cyber attack is unjustified, unfair and unhelpful.

Ladies and Gentlemen of the Commerce Committee….what you are dealing with here is the invention of gun powder….mandating thicker armor won't work just like building broader moats wouldn't stop invaders who had invented catapults & just like the Maginot line was no defense against the invading Germans in WWII.

We can't use 19th & 20th century models & federally regulating the Internet or giving DHS the power to make the final decisions about securing technology they don't own or operate will make our cyber security less effective. We need a much more contemporary and creative approach wherein the private sector is engaged, not controlled by our government partners. We believe the Task Force Report goes in the right direction and urge you to follow that approach.