Testimony of
Larry Clinton, President & CEO
Internet Security Alliance

before the
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Homeland Security Committee
U.S. House of Representatives

Hearing on
Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal

June 24, 2011

I. INTRODUCTION

Good morning Mr. Chairman, and thank you for inviting the Internet Security Alliance to testify before the Cyber Security, Infrastructure Protection and Security Technologies Subcommittee.

The Internet Security Alliance is a multi-sector trade association that develops best practices and standards, along with technological, economic and public policy services focused exclusively on cyber security.

ISA was founded and fully funded by a group of private sector entities in 2000. That's nearly 2 years before the tragic events of 9/11, 4 years before Congress created DHS, 6 years before DHS created its first cyber security Assistant Secretary, 7 years before they filled that position, 9 years before the President appointed his first "Cyber Czar" and 11 years before the President presented his first set of legislative proposals on cyber security to the Congress.

For more than a decade, the private sector has been taking a leadership role in the fight to secure cyber space. That is one reason we were delighted when President Obama addressed this issue from the White House and published the Cyberspace Policy Review shortly after taking office ----an enlightened document based on an extensive and wide ranging study by staff of the National Security Council.

II. THE PRIVATE SECTOR HAS BEEN AGGRESSIVELY ATTEMPTING TO UTILIZE THE PUBLIC-PRIVATE PARTNERSHIP TO ENHANCE OUR CYBER SECURITY

Over the past decade, ISA has testified approximately a dozen times before various Congressional Committees constantly urging, even pleading, for the government to take more aggressive steps to enhance our nation's cyber security. There may be some in the private sector that have suggested a hands-off role for the government in this space, but ISA is not one of them.

And, we are not alone. When legislation began heating up in the last Congress, we heard reports from policymakers that there were so many private sector entities that were interested in the subject that is was becoming difficult for our government partners to achieve clarity as to where the private sector stood on the issue.

As a result, several of the major associations involved in this debate banded together and worked over a period of six months to create a detailed ---26 page---white paper specifying our overall approach to cyber security and providing detailed policy recommendations.

This unique coalition, which included the Internet Security Alliance, the Business Software Alliance, the Center for Democracy and Technology, Tech America and the U.S. Chamber of Commerce is noteworthy for several reasons.

First, is the obvious size of the coalition, covering literally tens of thousands of companies. Second, is the breadth of the coalition. In the cyber security field, the "partisan divide" is generally between the providers of technology and the users of technology. This coalition included both. In addition, the civil liberties community is represented by the most active such organization in this space, CDT.

Finally, there is the depth of the coalition. It is not uncommon to see a coalition of this size in D.C.; however, they are usually brought together on a one or two page letter. In this case, we have produced an extended, and we think a cutting edge, detailed policy paper that analyzes a wide range of issues in the cyber security space and proposes specific policies---not just broad principles.

Moreover, we sought, as much as possible to be open with our government partners. We took as our starting points the official publications produced by our government partners: the National Infrastructure Protection Plan (NIPP) and the Cyberspace Policy Review released by President Obama in May of 2009. Central to both these documents is the need for the government to work in partnership with the private sector.

This realization has nothing to do with politics. It is based on the fact that in cyber conflicts, it is the private sector that is most likely to be on the front lines and it is the networks owned and operated by the private sector that provide the critical infrastructure ---both the regulated and non-regulated ones---upon which any modern nation relies.

Government does not have all the answers and often will not be the best judge of how to manage private systems. Altering our strategy to give the federal government final say over how private companies manage their systems will be costly, inefficient and ineffectual. Cyber security must be achieved through a true partnership between the public and private sectors. We specifically endorsed this foundation as embraced in these documents:

> "The current critical infrastructure protection partnership is sound, the framework is widely accepted, and the construct is one in which both government and industry are heavily invested. The current partnership model has accomplished a great deal. However, an effective and sustainable system of cybersecurity requires a fuller implementation of the voluntary industry-government partnership originally described in the NIPP. Abandoning the core tenets of the model in favor of a more government-centric set of mandates would be counterproductive to both our economic and national security. Rather than creating a new mechanism to accommodate the public-private partnership, government and industry need to continue to develop and enhance the existing one."[1]

In an attempt to develop our own policy proposals via the established partnership model, we not only notified the White House of our intent to create the industry White Paper, but reached out to them on a regular basis to keep them informed of our progress. We discussed the work at the forums established under the NIPP, such as the IT Sector Coordinating Council meetings, which are regularly attended by DHS staff. When the paper was completed, well prior to release, we sent a full copy to the White House for their review and comment. We requested, and eventually received, a one hour meeting at the White House to brief them on our proposals and requested ongoing interaction so that we could, as partners, come to a common ground on the way forward. Unfortunately, no subsequent meetings were scheduled and we were never briefed on the White House's own---substantially different---approach until it was released and sent to the Congress.

III. WE HAVE THE TOOLS TO STOP BASIC ATTACKS

The Committee is aware of numerous and varied cyber attacks. Indeed, the Internet is under attack all day, every day, and while we successfully deal with the vast majority of the attacks, we also must aggressively improve our cyber security.

---

[1] Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, TechAmerica; *Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper*; March 2011.

However, not all attacks are the same. Cyber attacks can of course be segmented many ways, but given the shortage of time, we can create two broad categories: one of basic attacks (which can be extremely damaging) and one of very sophisticated attacks.

Most cyber attacks fall into the first---the basic ---category. Although these attacks can be devastating from many different perspectives, they also are largely preventable.

Several different sources, including government, industry and independent evaluators, have concluded that the vast majority of these attacks ---between 80 and 90% --- could be prevented or successfully mitigated simply by adopting best practices and standards that already exist. Among the sources who have reported this finding, we can list the CIA, the NSA, PricewaterhouseCoopers and CIO Magazine.

Most recently, a comprehensive study jointly conducted by the U.S. Secret Service and Verizon included a forensic analysis of hundreds of breaches and literally thousands of data points and concluded that 94% of these, otherwise successful, cyber attacks could have been successful managed simply by employing existing standards and practices.

IV. WHY ARE WE NOT STOPPING THE BASIC ATTACKS?

Cost.

Some have suggested that the market has failed to produce the needed technology to address the cyber threat. That is not the case.

President Obama's own Cyberspace Policy Review documents the fact that the private sector has developed many adequate mechanisms to address our cyber insecurity, but they are not being deployed: "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."[2]

This finding is substantiated by multiple independent surveys that also identified cost as the biggest barrier to deploying effective cyber security solutions. This research shows that although many enterprises are investing heavily in cybersecurity, many others, largely due to the economic downturn, are reducing their cybersecurity investments.[3]

The fact is that many companies don't see an adequate ROI to cyber investments. This real world problem cannot be permanently wiped away by granting a government department the power to mandate uneconomic expenditures as President Obama himself pointed out last year at the White House: "Due to the interconnected nature of the system this lack of uniform implementation of sound security practices both undermines critical infrastructure and makes using traditional regulatory mechanisms difficult to achieve security."[4]

Rather, we need to find ways to work within the partnership to encourage firms to make investments that may go beyond their own commercial risk management requirements for security, but might rise to the level of a broader national interest. This principle was recognized in the creation of the original NIPP:

"The success of the [public-private] partnership depends on articulating the mutual benefits to government and private sector partners. While articulating the value proposition to the government typically is clear, it is often more difficult to articulate the direct benefits of participation for the private sector…. In assessing the value proposition for the private sector, there is a clear national security and homeland security interest in ensuring the collective protection of the Nation's [critical infrastructure and key resources] (CI/KR).

---

[2] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 31.

[3] PricewaterhouseCoopers, *The Global State of Information Security*, 2008.
Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2010

[4] White House, *Remarks by President Obama at White House Meeting on Cyber Security*, July, 2010.

Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CI/KR protection through activities such as:

- Providing owners and operators timely, analytical, accurate, and useful information…
- Ensuring industry is engaged as early as possible in the development of initiatives and policies related to [the NIPP]
- Articulating to corporate leaders …both the business and national security benefits of investing in security measures that exceed their business case
- Creating an environment that encourages and supports incentives for companies to voluntarily adopt widely accepted, sound security practices
- Providing support for research needed to enhance future CI/KR protection efforts."[5]

The Obama "Cyberspace Policy Review" went even further in suggesting this pathway by suggesting a mix of tailored incentives including liability incentives, procurement incentives, indemnification and even tax incentives.

The multi trade association White Paper continued this chorus of support for this approach.

"One of the most immediate, pragmatic, and effective steps that the government could take to improve our nation's cybersecurity would be to implement the recommendations made in the CSPR to explore incentives, such as liability considerations, indemnification, and tax incentives. For example:

- Tax incentives that encourage establishing additional cybersecurity investments, such as the R&D tax credit;
- Grant funding is used effectively in other homeland security areas such as emergency preparedness and response. Critical infrastructure industries can use grant funds for research and development, to purchase equipment, and to train personnel;
- Streamlining regulatory procedures, which would cut both government and industry costs;
- Updating the SAFETY Act to better appreciate the cyber threat that has become more evident since its enactment. This Act, which provides a mix of marketing, insurance and liability benefits for technologies designated or certified by DHS, can be expanded to standards and practices as well as technologies that protect against commercial as well as terrorist threats;
- Liability protections or regulatory obligations (e.g., for utilities) adjusting in numerous ways to provide incentives for enhanced security practices, such as adoption of standards and practices beyond what is required to meet commercial risks, or enhanced information sharing. Liability benefits do not need to be elevated to immunity to be attractive. Categories of liability (e.g., punitive vs. actual damages) or burden of proof levels (preponderance rather than clear and convincing evidence) can be adjusted to motivate pro-security behavior without costing taxpayer dollars; and
- Stimulating the growth of a private cyber insurance industry that can both provide private economic incentives to spur greater cybersecurity efforts while also creating a private market mechanism that fosters adoption and compliance. the government should give consideration to implementing reinsurance programs to help underwrite the development of cybersecurity insurance programs. Over time, these reinsurance programs could be phased out as insurance markets gain experience with cybersecurity coverage."

To accommodate the needs of a wide variety of critical infrastructures with different economic models, the public-private partnership should develop a menu of incentives that can be tied to voluntary adoption of widely-accepted and proven-successful security best practices, standards, and technologies. The R&D tax credit may be the most attractive option for an IT security vendor, while a defense firm may be more interested in procurement options, an electric utility in a streamlined regulatory environment, or an IT-user

[5] *National Infrastructure Protection Plan*, 2006 at 9.

enterprise in an insurance discount and risk transfer. Many of these incentives are deployed successfully in other areas of the economy, but not yet to cybersecurity."[6]

V. ADDRESSING SOPHISTICATED ATTACKS

While most cyber attacks are fairly basic and can be stopped or mitigated with the deployment of existing standards, practices, and technologies, which could be achieved through the use of a creative incentive system, there are still other much more insidious and sophisticated attacks that are not going to be stopped with best practices.

Again, there are many ways to characterize these attacks but one common term that has come to be used somewhat generically in the field is the Advanced Persistent Threat (APT).

Without getting into the academic debate over what constitutes the APT, it suffices to say these are sophisticated attacks. These are not "hacker kids" or kids in basements. These attacks are formulated by highly sophisticated, well organized, well funded, often state-sponsored attackers. These guys are pros. They are very good, and if they target you or your system you can be pretty sure they will succeed in penetrating, or "breaching" your system.

However, this does not mean we have no defense. Indeed, many companies have been working for several years with some success on mitigating APT attacks although it necessitates altering our defensive posture from one of perimeter defense geared to stopping breaches to internal detection and mitigation.

Again, the private sector White Paper identifies some of the current core strategies that the government, in collaboration with the private sector ought to be deploying to address the APT style (i.e., more sophisticated) attacks. However, it is important to note that there is no silver bullet to addressing these advanced threats.

The core reason we have attacks, and they will likely continue, is that the economic incentives generally favor the attackers. Many attacks are cheap, easy and profitable while on the other hand, an infinite perimeter needs defending, it is very hard to catch and prosecute cyber attackers and it is difficult to demonstrate ROI to things that you have prevented such as cyber attacks.

So long as our economic equation for cyber security remains out of balance, we are going to continue to have attacks. This needs to be understood not as a discrete problem for which there will be a simple and unchanging security technology—like a seat belt or a set of gold standard government metrics. Rather, this is an ongoing and persistent threat that needs continuous deployment of creative strategies that evolve with the dynamic threat.

VI. THE ADMINISTRATION'S LEGISLATIVE PROPOSAL

Unfortunately, after waiting two years for the Administration to follow up on its CSPR, we received a legislative proposal produced without coordination with the private sector partnership the Administration itself had established for this purpose, and which:

- Fails to follow up on the promise of earlier work by this and the previous Administration;
- Does not address the core economics issues which drive our lack of cyber insecurity
- Would create an extensive new bureaucracy that will not address the persistent cyber threats we face; and
- Could add significant new threats that are not justified by the dubious benefits of the unbounded intrusions into our most critical infrastructure

---

[6] Business Software Alliance, Center for Democracy & Technology, US Chamber of Commerce, Internet Security Alliance, TechAmerica; *Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper*; March 2011 at 10-11.

Since ISA works primarily with major entities from most for our nation's critical infrastructure, we will focus our testimony to Section 3 of the President's proposal, which establishes a new and extensive regulatory structure over the private sector.

VII. THE ADMINISTRATION'S LEGISLATIVE PROPOSAL FUNDAMENTALLY ALTERS THE PUBLIC PRIVATE PARTNERSHIP

When he released the Cyberspace Policy Review in 2009 President Obama himself said:

"Let me be very clear: My Administration will not dictate security standards for private companies. On the contrary we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."[7]

Unlike the rigorous and open process the Obama Administration conducted in developing the Cyberspace Policy Review, the current legislative proposal was not developed in any way by "collaboration with industry to find technology solutions."

ISA participates in numerous bodies set up under the NIPP to facilitate this sort of coordination including the Sector Coordinating Councils, the Cross Sector Cyber security Working Group, the Critical Infrastructure Partnership Advisory Council (CIPAC) and the Software Assurance Forum. Despite repeated requests for the Administration to engage with these bodies, designated by them for collaboration to develop solutions, there were no discussions at even a conceptual level about this proposal which would, if enacted, fundamentally alter the long standing relationship.

Had the Administration used the bodies designated for this sort of interaction, I believe the proposal would be both substantively stronger and politically more practical.

Notwithstanding the process, the centerpiece of the proposal –the establishment of an unbounded regulatory structure for the Department of Homeland Security - is obviously directly at odds with what the President pledged when he released the Cyberspace Policy Review two years ago.

Obviously it will be the the Committee and the Congress's decision whether to follow this new government centric approach, but there should be clarity at the very least that by establishing a broad regulatory framework, as this proposal does, it will fundamentally alter the nature of the relationship between the government and private sector.

It's often said that to a hammer, everything looks like a nail. And prisoners and prison guards do not have a partnership. One body is mandated to do what the other entity directs. While there is a fair amount of verbiage in the Administration's proposal about working with the private sector, as we will discuss shortly, at the end of the day, this legislative proposal will allow DHS to regulate pretty much any entity it elects to regulate and mandate whatever DHS elects ought to be mandated.

Some may argue that such a system of regulatory mandates will finally solve our cyber security problem; however, there is no evidence that this will be the case. Indeed, the academic research on motivating investment in information security specifically points in the opposite direction indicating that "proactive" investments motivated by market incentives are more effective than reactive (prompted by regulation) are.

A new study released from Dartmouth College earlier this month documents this finding, "Proactive investments are more effective at reducing security failures than reactive investments. When proactive investments are forced by an external requirement, the effect of the proactive investment is diminished …our results show that learning by doing through proactive security investments relies on economic incentives whereas unilaterally mandated procedures do not have any economic incentive…government

---

[7] *President Barack Obama, Release of the* Cyberspace Policy Review, *May 29, 2009.*

requirements simply focus attention on the problem area rather than discovery and learning by doing…external pressure does not have significant social incentives." [8]

VIII. THE ADMINISTRATION'S LEGISLATIVE PROPOSAL IS NOT SUPPORTED BY RESEARCH OR PRECEDENT

Research[9] has consistently shown that the single biggest barrier to enhancing the cyber security of our nation's critical infrastructure is economic. As previously mentioned, the National Infrastructure Protection Plan (NIPP)[10] identified the need for government to create a value proposition for industry to make investments in cyber security that are not justified by their business needs, but may be required for overall national security. In fact, the Cyberspace Policy Review specifically advocated the development of proactive market incentives such as procurement, tax and liability to incentivize additional cyber security investments.[11]

However, the Administration's legislative proposal does not follow through on any of these policy commitments.

Instead, the Administration's current legislative proposal relies primarily on "disclosure" as a market incentive, to hoping that reaction to such a public disclosure will generate increased cyber security investment. While at one point, this may have made sense; it is not likely to be helpful when addressing the current attacks we face.

IX. THE FOCUS ON DISCLOSURE OF BREACHES IS OUTDATED

Most cyber attack disclosure requirements are founded on misconceptions about what it is companies have available to disclose. Most sophisticated successful modern cyber attacks go undetected. Furthermore, cyber intrusions and malware, as they become more sophisticated and more damaging, become increasingly difficult to detect. The tools and services for detecting them are very expensive, and the evidence for their presence is often very ambiguous.

The fact that the proposed legislation and the discussions that surround it are constantly referring to "breaches" shows how rapidly policy in this field becomes dated. "Breaches" were the big cyber-security concern of the last few years, but they are not the big cyber-security concern of the era that began with Stuxnet. What's more, the very term "breaches" suggests that the remedy to cyber attacks is perimeter defense -- guarding the organization's information border against forces attempting to penetrate, or "breach" it. This is a way of thinking about cyber security that many of the foremost cyber-security experts have been arguing is obsolete for half-dozen years now. ISA presented this finding to the Obama Administration which cited the study in their Cyberspace Policy Review and published it on the White House Web site, but did not reference it in their own legislative proposal.

In fact, most companies are unable to tell whether they have been the victim of a successful 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 the annual evaluation procedure the Administration 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

---

[8] Kwon, Juhee and Johnson, Eric; *An Organizational Learning Perspective on Proactive vs. Reactive Investment in Information Security*. Dartmouth College, NH. June 2011 at 18.

[9] PricewaterhouseCoopers, *The Global State of Information Security*, 2008.
Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2010.

[10] The *National Infrastructure Protection Plan* (NIPP) is available at http://www.dhs.gov/files/programs/editorial_0827.shtm#0

[11] Executive Office of the President, *Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009.

degree of motivation.

X. THE ADMINISTRATION'S PROPOSAL CREATES THE WRONG INCENTIVES

Mandatory disclosure punishes companies that are good at detecting intrusions and malware. It creates an incentive not to know, so that there is no obligation to report. It diminishes the motivation of internal investigators, who may worry that finding out exactly what happened may do their company more harm than good. It adds to the ultimate costs of detection tools and services, making companies more reluctant to spend money on them.

Requiring companies to disclose their cybersecurity plans and certifications is, if anything, even more likely to have unintended consequences than requiring disclosures of successful cyber attacks. The kinds of language and administrative formulas that would be adopted to comply with such requirements would almost certainly have little to do with real cybersecurity. This is partly because the field is developing so rapidly that by the time cybersecurity plans were recognized as fulfilling administrative expectations, they would already be obsolete. There is also no way to tell at the level of a "general plan" whether the cybersecurity measures involved would be doing any good or not. The consequence of disclosing such plans would be another, costly level of administrative bureaucracy and auditors that would probably only be getting in the way of good security.

XI. ADMINISTRATION'S PROPOSED LANGUAGE PROVIDES DHS WITH UNFETTERED AND UNJUSTIFIED AUTHORITY OVER PRIVATE SYSTEMS

Although it has been suggested that the intent of this legislation is to cover only the most critical "core" infrastructure, a careful reading of the legislative language indicates that it provides essentially unfettered authority to DHS to mandate technical standards for almost any aspect of the private sector.

Sec 3 of the Regulatory Framework for Covered Critical Infrastructure lists a full page of requirements to be met before an entity is subject to these, as yet unspecified, federal mandates.

However, when reading through them, they don't provide any limit on the Secretary's authority to designate any enterprise as a so called "covered critical infrastructure" and thus subject to DHS mandates.

It's easiest to analyze the impact of the sections if we review them in reverse order.

Subsection D states that being named on the list as a covered critical infrastructure under this section "shall be considered a final action for purposes of judicial review."

Subsection C lists a variety of criteria to be placed on a "risk based tier," but criteria number 4 is "such other factors as the Secretary deems appropriate," which means the Secretary can place any entity on any tier for any reason he or she wants to.

Subsection B lists only 2 criteria for inclusion. One criterion is that the entity or system "is dependent on information infrastructure to operate."

Since virtually all modern systems that are reliant on some form of information infrastructure to operate, those criteria are all encompassing.

That leaves us only with the criteria listed section B1, which is that incapacity or disruption of the reliable operation of the system would have a "debilitating effect" on national security, national economy or national public health or safety."

We regard "debilitating" as a fairly loose, and frankly weak, criterion for conferring such broad authority to the Secretary. To "debilitate" simply means to weaken---it doesn't necessarily mean to weaken a lot ---just weaken. When I catch a cold I'm somewhat debilitated---but I wouldn't want the CDC to have the power to therefore regulate me.

According to this legislative language, if the Secretary decides, for any reason, that the incapacity of a system might in some way weaken our economy, security or safety, he or she has the authority to mandate ---as a final action--- whatever technical standards over their cyber systems the Secretary desires.

For example, the recent SONY Play Station attacks reportedly will cost more than a billion dollars in damage, which one can argue weakens or "debilitates" the economy at least somewhat. Would that then make SONY Play Station's "covered critical infrastructures" under this definition? When asked that question at a recent Judiciary Committee hearing, an Administration witness replied that that determination would have to be made through rulemaking under the Act.

In addition, the language does not state that the debilitating effect referred to in Sec (b) (1) has to be from a cyber incident. According to this legislative language, the fact that the World Trade Center was attacked with airplanes, which obviously had a debilitating effect on our security and economy, would be justification for DHS to impose mandates on the cyber systems operating in the WTC, even though they had nothing to do with the attack.

In addition, one criterion DHS will use in assigning an entity as a covered critical infrastructure is its interconnectedness with other infrastructures. That again allows for a tremendous expansion of potential DHS authority.

For example, the supply chain for weapons systems can be thousands of companies long. Obviously, interruption of the operation of these systems for whatever reason---including non-cyber reasons--affects our national security. So under this language, all these thousands of other companies would be potentially subject to DHS regulation due to their interconnection to the main weapons system project.

Moreover, under Sec B1 of this provision, DHS will regulate "entities" as opposed to systems or assets. This presumably means that an attack having a debilitating---however minor---effect on security, economy or health would result in the regulation of the entire entity the system is interconnected with.

The bottom line is that this legislative proposal provides almost unbounded discretion for DHS to classify an entity as covered critical infrastructure and subject the entire entity to unspecified regulation.

Section 9 states specifically that "the Secretary shall promulgate regulations...to carry out the provisions of the Title."

Section 2 states clearly that one of the purposes of the Act is to "establish workable frameworks for implementing cyber security minimum standards and practices."

Some may ask, "what's wrong with DHS establishing minimum standards for industry through a rule making." The problem is it won't work and it is substantially counterproductive.

Now, ISA is a big fan of standards and practices and we work with many entities, including NIST and other federal government agencies as well as private sector entities to create and constantly update them.

However, there is a major difference between using the existing consensus process to develop international standards and practices and having a government entity determine such standards and mandate them on the private sector.

The multi trade association White Paper addresses this argument in an entire section, concluding that:

> "[w]e have already seen that attempts to impose nation-specific requirements under the auspices of security are not embraced by the private sector or the civil liberties and human rights community for both public policy and economic reasons. A government-controlled system of standards development that resides outside the existing global regime will not be accepted. If imposed, it would quickly become a second-tier system

> without widespread user or technology community adoption, thereby fracturing the global network of networks and weakening its security."[12]

Again, although there is a great deal of verbiage discussing how the government will work with the private sector, the bottom line is that this legislative proposal consistently gives DHS massive new regulatory authority.

Section 7 requires CEOs to certify that they are in compliance with the plans required under the act. Although there is substantial verbiage suggesting that DHS will work with the covered entities in creating these plans, Section 8 empowers the Secretary to review any entity's plan, and if DHS finds the plan wanting for some reason, they are empowered to "take such action as the Secretary deems appropriate." In addition, paragraph 4 empowers the Secretary to evaluate the frameworks created through various discussions with the private sector. However, should DHS determine that the standardized frameworks don't meet their criteria, they are empowered to adopt their own framework to meet their criteria, and, thus, the DHS framework would be what a covered entity would be required to implement and certify.

XII. THE ADMINISTRATION'S PROPOSAL FOR EVALUATION IS ANTI-SECURITY

Under this proposal, an apparently enormous range of companies would be required to construct plans for cyber security and be required to hire federally approved "evaluators" to review their internal security on an annual basis. There is little if any evidence that regulatory compliance is per se improved security. Indeed, many report that compliance requirements distract personnel from security work to attend to the compliance regime.

Moreover, it is acknowledged on all sides that we face a critical shortage of qualified cyber security personnel, and so the army of evaluators created under this proposal will almost by definition not be adequately trained.

The single largest vulnerability of our cyber systems comes not from hackers using technology to break into systems, but from "insiders" with approved access to the systems. This proposal creates a virtual army of insiders crawling through our most critical infrastructure's security systems on an annual basis.

The threat of introducing constant stream of new "insiders" into our nation's most critical infrastructure far outweighs the dubious assumption that they will provide a tangible security benefit. That does not even account for the costs industry will bear to hire these evaluators, the cost of new manpower at DHS to comb through this mountain of data and the potential of an ideal attack vector where all these reports detailing our nations security will be stored.

XIII. THE INFORMATION GENERATED BY THESE DISCLOSURES WON'T ENHANCE SECURITY

Ironically, one of the unintended effects of more comprehensive or stringent disclosure laws could be less information about the sort of cyber attacks that really matter. This is because most of the mandated disclosures would simply be noise. There would be a constant stream of reports, based on what lawyers believe would demonstrate compliance, while actually revealing as little as possible. This stream of reports would obscure the attack trends that really matter, while allowing companies to conceal events that might otherwise provoke public outcry and more active government intervention. As cyber attack disclosures have become more frequent and more routine, this has already been happening.

The information made public by disclosure requirements is usually not very meaningful. Most cyber attacks, even if they are successful, do relatively little harm. They gather information that the attackers are never able to utilize. They provide one component of a larger attack program that never comes to fruition.

---

[12] Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, TechAmerica; *Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper*; March 2011 at p.8.

In many cases, the effects of the disclosure are considerably worse than the effects of the attack itself. The mere fact that a company has suffered a successful attack gives little indication of its actual losses, even if specific numbers are mentioned. This is because there are so many factors that can influence the scale of loss, including the wording of the disclosure itself. Determining how much a successful cyber attack will hurt a company is very difficult even for those who have access to all of the details of the attack, the operations affected, and the company's finances. For the general public, the bare facts of a successful cyber attack are often very misleading.

The cumulative data from the cyber attacks that have so far been publicly reported are also very misleading. Many of the biggest reported losses of personal data were due to lost or stolen laptops. This is not because it is the main way personal data is stolen; it is because the loss or theft of a laptop is an unambiguous event that it is hard not to acknowledge. Many of the other reported losses of data have been from major defense contractors. This is not because the major defense contractors are losing more data than other companies or than government departments; it is because they have the best detection systems in place. Some of the most publicized cyber attacks have involved Google mail. This is not because Google mail has been compromised more than other e-mail systems; it is because Google's business model depends more on trust and on certain types of transparency than the business models of the other companies providing e-mail services. Since most cyber attacks go unrecognized, the mere fact that a cyber attack is being reported means that it is atypical.

XIV. USING EFFECTIVE MODELS A) THE CDC

All of this does not mean that all disclosure laws or bad or even that the existing ones are bad. It merely points out the unintended effects of such laws that legislators need to make an effort to avoid in drafting additional laws. More information about cyber attacks in general and about the degree to which individual systems and companies are at risk is necessary for markets to take adequate account of these things. Disclosure laws could provide some considerable benefits. But they will not provide the intended benefits unless they take into account how systems are monitored for attacks and what additional information might be needed to put the attacks in context.

It is possible that the best approach might be to have the reporting go to a special legislatively created institution, rather than directly to the public. This is the model used with disease control and public health issues. With sufficiently clear instructions as to how this institution would handle the information, its actions could potentially be accepted by all parties. There are other ways disclosure could be handled that would be less crude in its effects. The point here is that any disclosure laws need to be framed with a conscious acknowledgment of the pitfalls.

XV. EFFECTIVE MODEL B) SEMATECH

In the 1980s, the United States also faced a technological onslaught. During this decade, the nation of Japan began flooding the U.S. market with computer chips, which threatened to drive U.S. chip manufacturers out of business. Recognizing the economic and security threat that this posed, the U.S. enacted legal measures such as the Federal R&D tax credit and the Cooperative Research Act of 1984, which eventually led to the private sector and U.S. Department of Defense cooperative known as SemaTech. Within two years, sub-micron architectures, advanced x-ray lithography and a number of other critical innovations pushed U.S. chip makers back in to world leadership, and produced generation jumps in computing capabilities just as the Internet was dawning.

A similar Cybersecurity Public-Private Cooperative could be composed of the private sector, academia and the government in a minority role. This organization could be charged with improving, even reinventing the cyber ecosystem in a more secure manner. Under this Cooperative’s umbrella, stakeholders could share information and cybersecurity technology development to create (or fund the creation of) more alternative networking protocols, software languages, and/or hardware architectures that are more secure. It could also act as an incubator for ideas to create better strategies to combat APT’s and their equivalent. It could also serve as the equivalent of an underwriters laboratory for cyber security by independently assessing best practices and standards along sliding scales. These proven increasing levels of security, if voluntarily

adopted, could then be used to qualify enterprises for subscribing to them in return for the incentive programs suggested earlier which will help mitigate costs while enhancing proven security practices.

The ISA, its members and partners are aware of the need to combat cyber threats---indeed that is why ISA was created over a decade ago. However, this must be done in collaboration with government, not as mandated by government. Moreover, the solutions we derive must be both technologically and economically practical if they are to have the sustainable effect we require.