The Internet Security Alliance

answer to the

Department of Commerce Green Paper: Cybersecurity, Innovation and the Internet Economy

August 1, 2011

Contact: Larry Clinton, President
Phone: 703/907-7090
Email: lclinton@isalliance.org

Recommended Definition of Internet and Information Innovation Sector (I3S):

The Department of Commerce should designate a new sector, called the Internet and Information Innovation Sector (I3S), to capture functions and services that fall outside the classification of covered critical infrastructure and have a large potential for growth, entrepreneurship, and vitalization of the economy. More specifically, the following functions and services are included in the I3S:

• provision of information services and content;
• facilitation of the wide variety of transactional services available through the Internet as an intermediary;
• storage and hosting of publicly accessible content; and
• support of users' access to content or transaction activities, including, but not limited to application, browser, social network, and search providers.

Questions/Areas for Additional Comment:

• How should the Internet and Information Innovation Sector be defined? What kinds of entities should be included or excluded? How can its functions and services be clearly distinguished from critical infrastructure?
• Is Commerce's focus on an Internet and Information Innovation Sector the right one to target the most serious cybersecurity threats to the Nation's economic and social well-being related to non-critical infrastructure?
• What are the most serious cybersecurity threats facing the I3S as currently defined?
• Are there other sectors not considered critical infrastructure where similar approaches might be appropriate?
• Should I3S companies that also offer functions and services to covered critical infrastructure be treated differently than other members of the I3S?

ISA Response:

The ISA is not supportive of the creation of the I3S.

This strikes us as an artificially created "sector" designed for governmental classification ease rather any legitimate economic or security needs.

Interestingly, the Internet is probably the least amenable area for government to construct artificial sectors. The sector model is outdated, and has been for decades. This in fact was one of the reasons

that when the ISA was founded 12 years ago we consciously rejected the sector model and opted for a non-sectoral approach.

Sectors historically define economic areas of interest (defense/agricultural/banking etc.). However all these sectors use more or less the same Internet and the same equipment. From an Internet security perspective it makes no difference if the 1s and 0s being stolen represent credit card numbers, the secret formula for Coke or national secret. The Internet is an inherently cross sector entity and security concerns need to be addressed on a cross sectoral basis. The department's desire to create a new sector for their own use is not justified or helpful.

The Green Paper offers no evidence that cyber security can better be achieved in the vaguely defined "critical sectors" as envisioned in the Administration's regulatory legislative proposal than in those that will presumably be lumped into I3S. As such there is no substantive evidence to require one set of entities to be subject to federal regulation while allowing others to operate via incentives. Absent evidence that regulation leads to better security than incentives, government should not be expanding its regulatory authority.

Instead, the pro-market incentive based solutions discussed in the balance of the Green paper ought to be applied to the currently unregulated economy. Portions of the economy that have intact regulatory structures can be used to enforce cyber security solutions as discussed below and metrics determining the relative effectiveness of the two approaches----incentives as opposed to regulation---ought to be then assessed.

While it may well be possible to come up with illustrative differences between companies in these two classifications it is just as easy to identify differences between entities within the classifications.

Moreover the Administration's legislative proposal defines entities covered under its regulatory structure at the corporate level. This does not match the modern evolution of enterprises many of which may have elements that are appropriately classified as critical while other portions of these same enterprises would be better understood as not part of the critical infrastructure (as most of the legislative proposals---apart from the Administration's---do).

Regulation and classification for regulation and classification sake is not helpful and is actually anti-security. What is needed is a flexible, evolving, and holistic approach to cybersecurity that doesn't rely on arbitrary classifications, but speaks to every business at the business plan level. Entities are too inter-connected to concentrate on just one group. A firm may make more than an adequate amount of investment in cybersecurity technologies and best practices only to be undermined by a connected entity that fails to do so.

As an example, assume a criminal or rogue state entity may desire to steal intellectual property from a high value target. Accessing the target directly may be difficult because the target organization has made substantial investments to prevent unauthorized traffic from entering its system.

However, since the Internet is characterized by broad interconnectedness the target entity may in fact be connected with other entities which have not made substantial investments. The criminal or rogue entity may attack this weaker element in the system and through that window gain access to the ultimate target.

Creating a new classification or categorization that addresses one possible segment of the cyber ecosystem, such as an "I3S," while failing to address the ecosystem as a whole will not solve this problem, known as "interdependent risk."

Policy Recommendation A1:
The Department of Commerce should convene and facilitate members of the I3S to develop voluntary codes of conduct. Where subsectors (such as those with a large number of small businesses) lack the resources to establish their own codes of conduct, NIST may develop guidelines to help aid in bridging that gap. Additionally, the U.S. government should work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices.

Questions/Areas for Additional Comment:
• Are there existing codes of conduct that the I3S can utilize that adequately address these issues?
• Are there existing overarching security principles on which to base codes of conduct?
• What is the best way to solicit and incorporate the views of small and medium businesses into the process to develop codes?
• What is the best way to solicit and incorporate the views of consumers and civil society?
• How should the U.S. government work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices?

ISA Responses

There is not only no need for the US federal Government to create its own standards, but creating nation-state specific standards is counterproductive.

AS ISAs has described in some detail (see Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress (2008) and Social Contract 2.0: A 21st Century Program for Effective Cyber Security (2009) government's role ought to be two fold. First government should establish and fund an independent authority---an underwriter's Laboratory---to test the various existing standards and practices for effectiveness. Second government needs to provide market incentives strong enough to generate economic motivation for entities to voluntarily adopt standards and practices that go beyond their commercial needs but may be justified investments from the national security perspective.

As the White Paper endorsed by ISA, BSA, Tech America, The US Chamber of Commerce and the Center for Democracy and Technology pointed out:

> "Indeed, many cybersecurity standards have been and are continually being established and updated through the transparent consensus processes of standards development organizations (SDO). Many of these processes are international in design and scope, and they routinely include active engagement by multinational corporations and various government entities that participate as developers or users of the technology. The multitude of continually evolving standards is essential because of the widely disparate configurations that are in use, and these configurations are constantly evolving and being updated to support rapid innovation in a dynamic industry. Both industry and government organizations voluntarily adopt the resulting best practices and standards that best fit their unique requirements, based on their roles, business plans, and cultural or regulatory environments. This historic process of standards development is widely embraced is highly participatory, and maintains high credibility in the global community. Not only does the standards regime facilitate interoperability between systems built by different vendors, it also facilitates competition between vendors that leads to greater choice and lower cost. Moreover, it spurs the development and use of innovative and secure technologies.

> Implementation of these resulting standards and best practices can also be highly effective in improving cybersecurity.
>
> An effective approach to cybersecurity policy needs to leverage this existing system of standards development rather than replace it with one that has a distinct bias in favor of agency or even national interests. We 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 communities for both public policy and powerful 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."

As mentioned previously, governments, either through national or international bodies, can serve an important security function by funding independent evaluations of the existing and emerging standards for their security effectiveness and applicability, and by working with industry to develop profiles of existing standards[1], as opposed to creating new standards or so-called "codes of conduct."

Naturally, varying standards formulas will provide differing levels of security and likely at different cost levels.

Moreover, the cyber networks and infrastructure constitute a global system where traditional borders do not apply. Not only are our companies and networks global, but so are our adversaries'. This global attribute must be taken into consideration for any policy or operational aspect of cybersecurity.

Any public policy deliberation must consider the impact of that policy on global competitiveness, interoperability, and compliance obligations. The companies that fuel our nation's economic growth are operating globally in one way or another. They either have business operations in many other countries, source their products and services globally, or rely on just-in-time delivery of components or products to meet their domestic customers' needs. Therefore, we cannot deliberate public policy with merely a segmented, national lens. Our nation's policy impacts the ability of its companies to do business globally, either directly through prescriptive restrictions or indirectly as a result of reciprocity or copycat policies in other countries.

Further, if U.S. policies raise concern about the level of government engagement in corporate networks or data as seems to be suggested by the above Department of Commerce recommendation and questions, it will raise skepticism by global customers regarding the U.S. government's access to their corporate or consumer data and the implications of that access. Customers will simply go elsewhere to find providers that do not pose the same concern. These potential consequences may not be apparent in any particular policy, but that makes it even more important that U.S. policy making consider the global impact of any proposed measure. The public-private partnership that forms the backbone of NIPP and the Administration's "Cyberspace Policy Review" recommendations, and which includes companies whose very existence demands a global perspective, needs to be more fully utilized to ensure that global impacts are considered from the beginning of a policy development process, whether in Congress or by the Administration

[1] Profiles are used to define how a standard will be deployed, and against which interoperability testing can be used to demonstrate compliance.

The partnership can also contribute to the international aspects of cybersecurity. It is important to build and foster global relationships that enable harmonization of appropriate policy mechanisms where they are needed and allow cross-border coordinated action on preparation and incident response on a sustained basis. The interaction of US-CERT with its counterpart computer security incident response teams (CSIRTs) helps foster that international coordination. We need to explore ways to integrate industry into those mechanisms as appropriate to further collaborative action.

As part of an international strategy, the U.S. government needs to find ways to leverage engagements with key allies and the global community (at varying degrees, as appropriate) to collaborate on improving situational awareness, analysis, and response, containment, and recovery measures. Current government-to-government efforts could be bolstered by new institutional arrangements or reduction of barriers to international coordination. In addition, such a strategy should articulate where in the international community the government should engage and with what position(s), and the role or efforts of the agencies engaged to ensure a consistent and coordinated approach. Because of its international engagement, the private sector has much to offer to these inter-government processes.

Given the importance of the global community in improving cybersecurity, the international component should be part of our national strategy. The CSPR specifically addresses this aspect and refers to the need to incorporate cybersecurity in our global diplomatic efforts. Not only can the U.S. reach out to global partners, but it can also provide capacity building that enables those countries to take measurable steps to improve their cybersecurity capabilities and become partners in the global effort to combat cyber attacks and cybercrime.

In order to develop and implement a cybersecurity diplomacy strategy, government needs to coordinate among its various components. In that regard, we applaud recent interagency coordination efforts and the establishment of a Coordinator for Cyber Issues to lead the Department of State's engagement on cybersecurity. There needs to be an early and ongoing partnership in order for both government and industry to leverage expertise, experience, insight, and relationships toward greater collaboration and success in the international environment. The global approach should include ways to foster even greater cooperation among law enforcement to more effectively pursue and prosecute cyber criminals.

Policy Recommendation A2:
The Department of Commerce should work with other government, private sector, and non-government organizations to proactively promote keystone standards and practices.

Questions/Areas for Additional Comment:
• Are the standards, practices, and guidelines indicated in section III. A. 2 and detailed in Appendix B of the Green Paper appropriate to consider as keystone efforts? Are there others not listed here that should be included?
• Is there a level of consensus today around all or any of these guidelines, practices and standards as having the ability to improve security? If not, is it possible to achieve consensus? If so, how?
• What process should the Department of Commerce use to work with industry and other stakeholders to identify best practices, guidelines, and standards in the future?
• Should efforts be taken to better promote and/or support the adoption of these standards, practices, and guidelines?
• In what way should these standards, practices, and guidelines be promoted and through what mechanisms?
• What incentives are there to ensure that standards are robust? What incentives are there to ensure that best practices and standards, once adopted, are updated in the light of changing threats and new business models?
• Should the government play an active role in promoting these standards, practices, and guidelines? If so, in which areas should the government play more of a leading role? What should this role be?

ISA Response

Identity assurance and credentialing are fundamental components of a cyber security program. Entities should use OMB 04 04 and NIST 800-63 to formulate an identity assurance framework. Identity is the foundation upon which a defense-in-depth program is built upon.

Authentication/ID Management aside, it should be noted that there is no set of gold or "keystone" standards. As previously mentioned, there are a multitude of standards and best practices designed for security purposes. This multitude is essential because of the widely disparate configurations that are in use, and these configurations are constantly evolving and being updated to support rapid innovation in a dynamic industry. Both industry and government organizations voluntarily adopt the resulting best practices and standards that best fit their unique requirements, based on their roles, business plans, and cultural or regulatory environments. Accordingly, an effective approach to cybersecurity policy needs to leverage the existing system of consensus-based standards development previously described rather than replace it with one that has a distinct bias in favor of national or agency/department interests.

The key issue for the Department of Commerce and government as a whole ought not to be whom or where the standards and practices are developed, but how well they work.

Mechanisms to determine efficacy (i.e., what works), for standards promotion, and incentives are detailed more fully in following sections.

Policy Recommendation A3:
The U.S. government should promote and accelerate both public and private sector efforts to research, develop and implement automated security and compliance.

Questions/Areas for Additional Comment:
• How can automated security be improved?
• What areas of research in automation should be prioritized and why?
• How can the Department of Commerce, working with its partners, better promote automated sharing of threat and related signature information with the I3S?
• Are there other examples of automated security that should be promoted?

ISA Response

In today's cyber security environment there is one inescapable truth. There is no way to prevent a determined intruder from getting into a network so long as one allows e-mail and web surfing –and no business today can survive long without these two bedrocks of the information age.

The reasons for this are simple. The vast majority of our Information Assurance architectures rely on patching and configuration control for protection, the consistent application of which has thus far proven elusive over large enterprises. It also relies on signatures for both protection and detection which, by definition, will not stop the first wave of the increasing volume of zero day attacks we are seeing today. Therefore, when you must let the attack vector (an e-mail or a web address) past your perimeter to the desktop, you are virtually guaranteed to have successful penetrations.

Moreover, the gaping hole in cyber collaboration (often called information sharing) is that the vast majority of small and medium–sized organizations, both commercial and government, do not participate in these groups or do not have the resources to take advantage of this information when they get it. Unfortunately, for many in critical infrastructure sectors, these small and medium-sized organizations represent a significant portion of our supply chain. We have a vested interest in their success.

Government ought to create a National Cyber Threat Protection Service to implement an automated disruption strategy that is more suited to the sorts of attacks most businesses and governments experience today. This more contemporary and automated model of information sharing will result in a vast increase in the number of enterprises who will receive—and will use---actionable information. It is built on a voluntary process supported by incentives at all levels to make the system function.

The best way to address the new reality of cyber attacks is to recognize that attackers will get into your network and reformulate our defensive actions to detect, disrupt, and deny attacker's command and control (C2) communications back out to the network.

The strategy is an acknowledgement of the fact that there are fewer, and relatively noisier, ways to get out of a network than to get into it. Such a strategy focuses on identifying the web sites and IP addresses that attackers use to communicate with malicious code already infiltrated onto our computers. While some of these sites are legitimate sites which have been compromised, the majority are usually new domains registered by attackers solely for the purposes of command and control. There is little danger of unintended consequences from blocking these web sites and their associated IP addresses for outbound traffic. Where they are legitimate sites, the benefit of protecting the enterprise far outweighs any inconvenience there might be if an employee needs to legitimately go to that site.

This strategy can be successful, but it requires a significant investment, unaffordable to most small and medium size entities and many larger ones.

One of the corollaries of recognizing that networks can always be penetrated is a shift in how we measure ourselves. Measuring ourselves against how many intrusions occur becomes a far less interesting. What counts, instead is the intruder's dwell time in our network, or how long an intruder has had access. It's more important to recognize how successful the penetrations were versus how many penetrations occurred. The ideal goal would be to have advance notice of a new malicious C2 channel so that even if someone opened a malicious e-mail the outbound C2 channel would already be blocked—making the effective dwell time zero.

There are two ways to reduce the dwell time of an intruder. The first is to make a considerable investment in traffic analysis and analytical methods to detect the malicious outbound traffic in a network. Some large organizations have had considerable success in this arena but it has required a large investment that a majority of organizations are not likely to match.

However, the other way to reduce dwell time is a method every organization, large and small, can match--collaboration with other operational entities. If we can take advantage of the good work of other organizations, we are eager to do so. We recognize that many other organizations regularly find and report C2 channels. Anti-virus vendors, CERT CC, managed security service providers, defense contractors, research institutions, intelligence agencies, other large government agencies, and law enforcement all see relatively narrow aspects of the C2 environment. But put them all together and they collectively see a very wide swath of the C2 threat environment. Many already aggregate and share the information formally or informally through ISACs, the Defense Industrial Base Cyber Task Force, Infraguard, or any number of other forums. But there is no central clearing house for this information or an operationally focused framework for rapid dissemination of this threat information to a broad national audience.

While there is no national-scale framework in place, there is a model that has already proven effective fighting other cyber security problems. The model involves a set of trusted entities developing threat information and reporting voluntarily (with non-attribution) to a central source, which consolidates the information and rapidly disseminates it to a very large user community. The user communities, in return, implicitly trust the centralized service and expend little or no resources to validate the information. They simply let the automated processes protect them as a passive service rather than investing in active collaboration—and with much better results.

If this sounds familiar, it's because it is the model used for the highly successful anti-virus and spam filtering industries. We propose that this same model be used to disseminate information on attacker C2 URLs and IP addresses and automatically block <u>outbound</u> traffic to them. If attackers get into your network but cannot get back out the attack is effectively thwarted.

Such a model will have a tremendous impact against botnets and the Advanced Persistent Threat (APT) both of whom make heavy use of web-based command and control. While the first wave of their attacks might initially succeed they would be short-lived after the first discovery because of the rapid and automated dissemination of the C2 channels. Subsequent waves would fail completely by virtue of rapid dissemination and automatic blocking of the C2 mechanisms. Of course, one could argue that an attacker could always rapidly change their command and control channels and make them unique to each attack. While this is true, the more we force intruders into greater costs and complexity, the more

likely we are to change his cost-benefit calculations. It seems axiomatic that anything that is both simple and inexpensive while forcing this behavior is worth doing on our part.

AN INDUSTRY-GOVERNMENT COOPERATIVE MODEL FOR DISRUPTING MALICIOUS CYBER COMMAND AND CONTROL

There are three types of entities involved in this process:

1. Threat reporters discover and report malicious C2 channels.

2. One National Cyber Threat Response Center (NCTRC) that acts as a central threat clearing house, collecting the threat reports, vetting them as necessary, and providing them to vendors in a standard format.

3. Vendors for firewall devices (the term here being used in its most generic sense) would accept the new threat information and push it out to their devices in the field the same way anti-virus and spam filtering vendors push new definitions today.

CERTIFIED THREAT REPORTERS

Threat Reporters are organizations with the detection and analytical capability to discover command and control sites via malware reverse engineering or traffic analysis. Organizations, be they commercial, private, or governmental, would apply to be certified as Threat Reporters and have their reports of C2 channels accepted as valid.

Some third party, presumably a government entity, an industry consortium or some hybrid of the two, such as, the described SemaTech model, would be responsible for certifying potential Threat Reporters against a moderate standard of in-house capabilities. The standard would measure both quality and quantity. Quality would be evaluated by a review of in-house detection and analytical capabilities designed to give *a priori* confidence in their reports' reliability. This would ensure the information the reporters provide is credible and allow for a more rapid automated dissemination process with minimum manual review. Quantity would be measured after certification to ensure the reporter was contributing enough unique threat information to the community to continue to merit the marketing advantage of being a Certified Threat Reporter.

It is important to note that submission of reports by Threat Reporters would not be the same as disclosing breaches required under other laws or agreements. A significant percentage of reports would come from intelligence or other detection activities not associated with any activity within the reporting organization's network. For this model to be viable the reporters have to be free to provide threat information without any implication that they experienced a breach or might get requests for involuntary disclosure of additional information.

Threat reporters would normally submit only malware command and control information, either web sites or IP addresses and the class of threat (e.g. botnet, advanced persistent threat, etc). That information, alone, is enough to make this model work if all parties trust the credibility of the assessment. Other detailed information on the malware involved could be voluntarily submitted, but not at the expense of rapid submission of the C2 channels.

The advantage to the Threat Reporters, especially managed security service providers, is in their ability to use the certification for branding purposes. Organizations that develop threat data internally but

which do not wish to participate due to low risk tolerance or because they feel reporting might conflict with their business model would simply not apply to become Threat Reporters.

NATIONAL CYBER THREAT RESPONSE CENTER (NCTRC)

The role of the NCTRC is to serve as a clearing house for processing reports of C2 URLs and IP addresses from Threat Reporters and rapidly distributing them to the community of firewall device vendors. By having a central point disseminating the information to all vendors equally we avoid the problem we face with anti-virus today where not all vendors detect all threats. The NCTRC would also de-conflict erroneous reporting that resulted in disruption to legitimate activities. The NCTRC would maintain a "reputation index" (e.g. credibility rating) for each reporter much like seller ratings on eBay. By this feedback loop a Threat Reporter could be decertified (i.e. no longer have their reports accepted or be able to claim Threat Reporter status in their marketing).

The NCTRC must be a single organization focused on rapid dissemination of actionable information. Unlike the current anti-virus business model where organizations submit malware to their vendor of choice, there would be only one clearing house. The question of who operates the clearing house is largely irrelevant so long as everyone in the model trusts them. It could be a government entity or, more likely, a non-profit organization overseen jointly by the government and an industry consortium. Regardless of who operates the NCTRC, the government must be as secure reporting information to it as industry is. With the large amount of IP threat information the government sees simply because of the size of its network, the absence of threats detected in their networks would significantly reduce the value of the model.

FIREWALL DEVICE VENDORS

Producers of devices that are capable of blocking outbound web traffic would accept the data from the Clearing House, reformat it as appropriate for their device, and push it out to their customers as quickly as possible. Traditional desktop or network firewalls, web proxies, and routers would all be capable of performing this function, thus giving network owners a wide variety of products from which to select based on their architecture and investment tolerance. The vendors would differentiate themselves from each other not only on price, but also on their speed of updates and value-add services such as the ability of their customers to manually override the lists or their ability to provide reports to network owners.

INDUSTRY AND GOVERNMENT BENEFIT

The real benefit from this model lies with the vast majority of network owners in business, industry, and government who cannot afford the deep detection and analytical capability needed to protect themselves. Today, these organizations are totally at the mercy of a determined intruder who is virtually guaranteed to be able to compromise systems with socially-engineered zero-day attacks. Most simply do not have the investment dollars to build a detection infrastructure dependent on traffic analysis or the expertise to make use of the various information sharing groups. With this model, though, these businesses could easily, and voluntarily, afford a single device that most already have anyway.

It would, however, now provide an order of magnitude increase in the level of protection by stopping in near-real time many of paths an attacker would use to get back out of the network. For those who had not been compromised yet when updates come out, they would completely nullify any subsequent attack with that command and control channel. For those who had already been compromised in the first wave of a zero day attack, it would minimize the length of time when an attacker could access the

compromised box and it would identify compromised computers that might otherwise have gone undetected. Best of all, assuming they implicitly trust the system, the organizations employing the model do not have to invest any additional resources to take full advantage of the model.

A secondary benefit would accrue to organizations whose websites have been hijacked and used as C2 sites (as opposed to dummy domains registered specifically for C2). These organizations would become aware of the infection more quickly as hits on their web sites dwindled or simply monitoring the NCTRC lists. They would be then able to exhibit good internet citizenship by quickly cleaning their systems and working with the NCTRC to be removed from the block list.

A third benefit, although perhaps more appropriate to a follow-on effort, would be the ability to tie the reported C2 channels to a library of instructions for finding and cleaning the specific malware where is was detected. This would be a much more complex and less automated process, but it would give smaller organizations a quick way to not only know they have a problem, but also allow them to short circuit the remediation process.

THE PROSPECT OF A COMMON OPERATIONAL PICTURE

Perhaps one of the most tantalizing side benefits of this model is that it could be the basis of a true Common Operational Picture. If every firewall device supporting this model not only blocked the outbound traffic, but also—again, voluntarily—reported back to the Clearing House that there was a blocked C2 attempt from their IP address it would, given the potentially hundreds of thousands of devices reporting in, represent a very accurate picture of the scope of any given attack or campaign. Unlike today when organizations are loathe to report incidents because of the risk of bad publicity, data reported to this COP would not reveal any information beyond the fact that someone on their network tried to communicate with a bad URL or IP. Plus, by definition, if the firewall device blocked the outbound traffic, the attack failed or has been neutralized. But knowing the nationwide scope of attacks from the same source would yield invaluable information unavailable today.

If the IP addresses reporting in could be grouped by their critical infrastructure or agency, the COP could be filtered to that organization. For example, if the NCC knew the IP space of all nuclear power plants, a COP could show attempts to access the same C2 sites from multiple power plants. This might indicate a concerted effort to compromise the plants. Similarly, the defense industry or financial community would see the scope of attacks across their community. Or the Department of Defense would see which attacks were unique to them since there might be no detections of specific C2 sites outside of DoD IP space. And all this in near-real time.

INCENTIVES

This model for denying and disrupting attacker command and control on a national scale includes positive incentives for every participant.

1. Organizations, especially commercial entities, will have an incentive to be certified threat reporters for branding purposes. It shows that they have a robust, capable process and investments to become credible reporters of threat data. There could even be tiered levels for branding purposes based on the volume and accuracy of inputs, i.e. an anti-virus vendor who might report a lot of C2 URLs based on all the malware they get would be Platinum Reporters. A large company with robust internal capabilities might be a Gold level. Managed Security Service providers would be especially eager to participate since the number of C2 channels first reported by them would be a tremendous marketing tool.

2. The Government will greatly benefit by being provided a very large body of C2 URLs and IPs with very little investment on their part. They will also benefit, of course, by the overall increased security of the industrial base which is a major goal of US policy. Most important, however, is the promise of a near-real time common operating picture that truly reflects the current threat environment. The main burden on the government's part would be the upfront effort to champion implementation and develop interface standards for receiving reports and disseminating them to vendors.
3. Firewall device vendors will have a great incentive to participate. They will be noticeable by their absence if they don't participate and it will most likely open up a whole new class of customers who see in a single device a high payoff defensive measure.
4. Best of all, small and medium sized organizations of all types will now have a way to take collective advantage of the investigative work of the best IA organizations in the country. By investing only in the firewall device that best fits their architecture, their security will increase by an order of magnitude or more simply because, like AV, a known bad domain will get blocked within hours of discovery.
5. This would also help to restore trust in the internet by identifying and isolating ISPs that do not maintain standards of good behavior on their networks. Their IP space and registered domains would frequently be blocked, presumably reducing their profitability and providing an incentive to good behavior.
6. Once this model is up and running it could easily be extended internationally. In fact many foreign producers would have a great incentive to have their devices capable of participating in this model. From there it is a short jump to an international model.

RISKS

The main risk associated with this model is the risk of blocking a legitimate web site that has been taken over by an attacker for use as a Command and Control site or downloader site. While we believe this risk will be small compared to the gain, the model envisions a reclaim or de-confliction process whereby a domain owner could get his domain removed from the list either as an error or after demonstrating his site was no longer hijacked. A secondary mitigation would be for the vendors to allow manual overrides on blocked domains at the local level, exactly as is done today with exceptions to web proxy vendors' predefined categories.

There is a secondary risk involved in building the trust relationships required to make this model work. Industry and government alike must be assured that there is no negative connotation to submitting threat data. The simple imperative of getting malware command and control data out to the broadest possible audience must take precedence.

Summary

This model, if implemented on a national scale, has the potential to be a game changer. For every attack, if a single organization discovered the attack, the entire nation would soon be protected. It would force an attacker to make the command and control channel unique for every attacked IP address. An attacker would have to either reduce the scope of attacks or greatly expand his domain registrations. In the later case, someone registering enough domains to operate on the level our attackers operate today would soon gain such a high profile they would be susceptible to other mitigations.

In the end, this model takes the best aspects of today's anti-virus, spam filtering, and proxy URL categorization to build a fourth service that is akin to anti-virus on outbound traffic. This National Model for Disrupting Attacker Command and Control proposed in this paper could set a new standard for effective public-private partnership in the Internet Age.

Policy Recommendation A4:
The Department of Commerce, in concert with other agencies and the private sector, should work to improve and augment conformance-based assurance models for their IT systems.

Questions/Areas for Additional Comment:
• What conformance-based assurance programs, in government or the private sector need to be harmonized?
• In a fast changing and evolving security threat environment, how can security efforts be determined to be relevant and effective? What are the best means to review procedural improvements to security assurance and compliance for capability to pace with technological changes that impact the I3S and other sectors?

ISA Response

As the above questions indicate, supply chain security is critical to cybersecurity. Without appropriate assurance that technology products and services are not counterfeits, are reasonably free from intentional and unintentional vulnerabilities, are appropriate to the level of threats they face once deployed, and are correctly configured and maintained, there can be little confidence that the information and communications they process and store are safe and secure.

Supply chain security is another area of cybersecurity policymaking and operations that requires that both government and industry leverage international industry best practices and standards, as well as work in a close public-private partnership. We believe such a partnership is needed to assure appropriate levels of security in the supply chain while transcending national boundaries, being economically practical, and including appropriate market incentives. As information technology is developed on a global basis, our approach to supply chain security must also be global and not segmented by agency or arbitrary classification.

Potential risks differ across sectors and throughout the development life cycle. Therefore, each actor in the life cycle has different risk management responsibilities. The public-private partnership can help them better discharge their responsibilities.

Technology suppliers have a responsibility to develop and deliver solutions that meet the needs of their global customer base and are worthy of its trust. To this end, the providers have contributed to the development of a wide spectrum of best practices and standards, as well as their own company-specific practices and controls. Assurance and inspection processes should be in place to verify product trustworthiness. The partnership has two important roles in that regard:

- Standards for assurance are developed through a multi-stakeholder international partnership framework rather than setting country-specific assurance standards, the government should expand its participation in the international standards-setting process;
- The public-private partnership should also facilitate on-going identification and dissemination of effective international assurance standards and best practices.

Finally, as recommended by the CSPR, the government, and its agencies, such as the Department of Commerce, can make another contribution to the supply chain security efforts of technology providers by sharing specific and actionable threat information with them, to help them address such threats and

improve their supply chain and technology design and development processes.[2]

Acquirers of technology also have an important role to play. The selection of specific supply chain risk management practices varies depending on the role of the IT system and how critical the IT element is within the system. Technology acquirers need to evaluate their suppliers' practices on the basis of recognized industry standards and best practices. They also have a responsibility to follow recognized best practices as they configure, integrate, deploy, and maintain technology solutions.

Acquirers of technology should actively leverage tools and resources available to ensure that they do not acquire counterfeit technology products. IT suppliers, especially commercial–off-the-shelf (COTS) vendors, have been fighting a sustained and costly battle against counterfeit products for decades. The Department of Commerce and the government as a whole should work in close partnership with industry to establish best practices that ensure the acquisition, integration, implementation, and use of genuine and legitimate products throughout the life cycle of systems. This includes leveraging commercial anti-piracy and anti-counterfeiting technologies and processes and putting in place more rigorous requirements for the government to purchase only from authorized dealers and resellers.

Providers of technology products and services implement a wide spectrum of international standards and best practices, as well as company-specific practices and controls so that their technology solutions deliver appropriate levels of security. Mandating country-specific, government-created risk management practices limits the user's access to cutting-edge technologies, causing several negative effects:

- A lack of measurable increases in security. For example, government has made attempts to require technology providers to share information that contains intellectual property and other trade secrets. Few if any acquirers have the appropriate level of technical expertise to make decisions based on such information, while suppliers would experience significant harm if that information's confidentiality was compromised.
- Government mandates evolve at a slower pace than technology; therefore, they compromise innovation by freezing design, development, and supply chain risk management practices in time and hampering related economic growth.
- Disparate and redundant government requirements regarding supply chain security would weaken security, because resources that would otherwise go to improving security would be assigned instead to complying with multiple standards.
- Mandates that are fundamentally at odds with recognized industry best practices and international standards restrict companies that build solutions for a global marketplace. As a result, such mandates greatly hinder competition between vendors, leading to fewer choices and higher costs. They would also open the door to imposition of other, divergent requirements by foreign governments. These effects would harm America's competitive position in the global marketplace.

Over the past few years, the Internet Security Alliance has sponsored and organized a massive project dedicated to finding more cost-effective ways to secure the global electronic supply chain. The project,

---

[2] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009 at 35.

which began in the fall of 2007, has involved three national conferences and a half dozen major workshops, as well as large numbers of meetings, interviews, and conference calls. It has had extensive participation by Carnegie Mellon, the U.S. Cyber Consequences Unit, and a large portion of the world's leading electronics companies.

The project had three major goals. The first was to find ways to protect global electronics companies from the major losses they have been suffering, due to delays in production, corruption of outputs, damage to reputation, counterfeiting, and the theft of competitively important information. The second goal was to find economically viable ways of stopping malicious firmware from being inserted into military and critical infrastructure information systems. This is a major concern, but there is no way economically viable way to solve it on its own. The third goal was to help open up the global electronic supply chain to more entrants, fostering a more geographically diverse and, hence, more stable and resilient supply chain.

The project culminated in a set of concrete security guidelines, describing specific security procedures for each stage of electronics production. The guidelines are fairly lengthy, because of the complexities of modern electronics manufacturing and its distribution across many locations. They are, however, eminently practical, because the number that apply at a given production stage is actually relatively small, and because they have all been carefully selected for cost effectiveness. Altogether these guidelines constitute the most comprehensive guide that has even been produced for manufacturing security in the electronic industry. This makes them an historical landmark and gives them considerable technical interest. They are intended be used as a reference document in the drafting of contracts between the producers of electronics products and their suppliers. They should serve to coordinate security throughout the electronics supply chain and provide a common standard that competing bidders can be expected to meet. The overall result should be a more efficient, fairer, and more resilient electronics supply chain, with lower risks for every participant

Policy Recommendation B1:
The Department of Commerce and industry should continue to explore and identify incentives to encourage I3S to adopt voluntary cybersecurity best practices.

Questions/Areas for Additional Comment:
• What are the right incentives to gain adoption of best practices? What are the right incentives to ensure that the voluntary codes of conduct that develop from best practices are sufficiently robust? What are the right incentives to ensure that codes of conduct, once introduced, are updated promptly to address evolving threats and other changes in the security environment?
• How can the Department of Commerce or other government agencies encourage I3S subsectors to build appropriate best practices?

ISA Response

Research shows that in general there are not sufficient economic incentives for the vast majority of enterprises to even maintain their current investments in cyber security notwithstanding the dramatically increasing threat. In fact surveys by PricewaterhouseCoopers and McAfee/CSI reported that investment in cyber security was deferred or reduced in between half to 2/3 of American companies in 2009 and 2010.

This applies across the board, and, accordingly, what is needed is an incentive based approach not only to "I3S," but to the entire cyber ecosystem.

There are three main issues that must be addressed in designing a system to create the sufficient incentives for businesses to make cyber security investments not currently justified by their business plans.

1. A mechanism must be developed to determine what sort of behaviors merit incentives
2. Incentives powerful enough to change the behavior of the specific business organizations must be made available to entities who adopt the desired behaviors
3. Mechanisms to assure that incentives are not fraudulently accessed must be developed

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.

Today, there are multiple sets of standards and best practices designed for security purposes. Some of the standards and practices are developed by government entities such as NIST, some by standards setting organizations such as ISO or ANSI and still others set up by smaller and more discrete entities. One reason for the multitude of standards and practices is that there are multiple different systems and configurations of systems and these systems exist for varying purposes operating in various cultures. No one size of standards or practices "fits all."

The key issue for government ought not to be whom or where the standards and practices are developed, but how well they work.

Private entities could apply for varying levels of incentive based on their use of increasingly higher levels of practices with greater incentives for more stringent processes, e.g., protection from punitive damages for adoption of a class "A" effective set of practices and higher burdens of proof for a higher graded level, etc.

There are already a number of incentives the government uses to promote pro-social action in areas like the environment, agriculture and transportation which can be adapted for use to promote good cyber security behavior, which can be readily applied here to drive cybersecurity enhancements. Among these devices are:

- Streamlined Regulatory Requirements and Elimination of Audit Redundancies – Discussed below
- Liability Benefits - 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.
- Insurance – Discussed below
- 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;
- Government Procurement – Discussed below
- SBA Loans – Tie SBA loans to adoption and implementation of cybersecurity best practices and technologies
- Stimulus Grants - Grant funding has been 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.

- Tax Incentives - Tax incentives that encourage establishing additional cybersecurity investments, such as the R&D tax credit

It is important for government to offer a wide range of incentives as certain categories will be more relevant to discrete organizations. For example, defense contractors or communications providers may be very interested in procurement advantages while small businesses may be more sensitive to liability benefits.

In addition, many of these incentive categories can be applied in multiple ways. As previously mentioned, liability benefits can range from immunity to simply alterations in burden of proof, and insurance benefits can range from qualifying for the ability to purchase a policy, through applying various discounts to programs for the adoption of carrying levels of security.

The final major aspect is to develop mechanisms to assess compliance with the provisions which merit the market incentives.

For regulated sectors such as chemical, energy utility and telecommunications the existing regulatory structure can be adapted to assess compliance.

The second such mechanism is liability. An entity that applies for an incentive and still has a breach could be found liable for fraud in applying for the incentive.

A broader mechanism to assist with the assessment of compliance with designated effective cyber security behaviors would be a more vibrant cyber insurance industry. As will be discussed in greater detail below, broader deployment of cyber insurance not only allows a mechanism for promoting good practices, but also provides a private sector funded mechanism for assessing compliance. When insurance companies have their own money on the line they have an enormous economic incentive to assure that the practices they are insuring are in fact being followed which has the concomitant societal advantage of further assuring better cyber security.

In sum, 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.

• *How can liability structures and insurance be used as incentives to protect the I3S?*

ISA Response

With respect to limited liability structures and insurance, such incentives should be available to not only the "I3S," but industry as a whole.

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 vs. clear and convincing evidence) can be adjusted to motivate pro-security behavior without costing taxpayer dollars

The federal government can also promote cybersecurity efforts by creating a Cyber Safety Act that provides safe harbors or other limitations on cybersecurity liability, contingent on reasonable efforts to

conform to best practices. This would provide a powerful incentive to adopt effective security measures. It would also make the regular security evaluations especially valuable. Precedent for this action may be found in the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, which provides limitations on liability and damages for claims against sellers of anti-terrorism technologies arising out of the use of anti-terrorism technologies, contingent on having liability insurance. The current SAFETY Act, while technically applying to cyber-terrorism events, is inadequate when applied to cyber-risk for a number of reasons: (1) the ability to connect a cyber-event with a terrorist group or hostile nation is, as a practical matter, almost impossible absent an admission on the part of the terrorist group, (2) the economic impact of a major cyber event is the same regardless of whether the event is terrorist related, criminally related, a result of negligence on some company's or individual's part, or (most unlikely) of unknown origin.

Nevertheless the SAFETY Act law and language can be used as a good template for legislation seeking to promote best practices in the area of cybersecurity by using the very effective "carrot" of limited liability in well outlined and monitored circumstances.

With a broader insurance market we can off-load much current government risk to the private sector. Moreover, insurance (discounts) are a major motivator of all sorts of pro-social behavior from smoking reduction to improved driving and building safety. ISA has done a fair amount of work on how to use insurance better ranging from some relatively immediate items such as sharing information leading to lower rates and greater uptake (due to more realistic risk assessments and pricing) to broader programs dealing with national re-insurance. This is discussed below.

Cyber insurance can improve overall cyber security. Cyber insurance increases cyber security by encouraging the adoption of best practices. Insurers will require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber-security.

The security requirements used by cyber insurers are also helpful. With widespread take-up of insurance, these requirements become de facto standards, while still being quick to update as necessary. Since insurers will be required to pay out cyber losses, they have a strong interest in greater security, and their requirements are continually increasing.

As well as directly improving security, cyber-insurance is enormously beneficial in the event of a large-scale security incident. Insurance provides a smooth funding mechanism for recovery from major losses, helping to businesses to return to normal and reducing the need for government assistance.

Finally, insurance allows cyber-security risks to be distributed fairly, with higher premiums for companies whose expected loss from such risks is greater. This avoids potentially dangerous concentration of risk while also preventing free-riding.

PROBLEMS WITH THE MARKET FOR CYBER-INSURANCE

Despite the benefits of cyber-insurance, the market for cyber-insurance is adversely affected by a number of problems.

First and foremost, insurers are afraid of a "cyber-hurricane" – a major disaster resulting in great number of claims. Cyber-hurricanes represent an uncertain risk of very large losses, and as such are

very difficult for insurers to plan for. Because computer systems are interdependent and standardized, they tend to be especially vulnerable to correlated losses of this nature. This fear increases insurance premiums, because insurers naturally focus on worst-case estimates of the expected loss from such an event so that they can maintain underwriting profitability. In addition, "cyber-hurricanes" raise a barrier to entry to the insurance market, because an insurer may be wiped out if a major event occurs before they have built up sufficient cash reserves. Prices for private market reinsurance for cyber-insurers is extremely high as the fear of a "cyber-hurricane" is felt most by the reinsurance community.

Second, although cyber-insurance has been around for more than 10 years, it is still considered a relatively new area and thus insurers are hampered by a lack of actuarial data with which to calculate premiums. In addition to increasing price, a lack of data leads to problems with the risk analysis undertaken by companies when deciding whether insurance against a particular risk is worthwhile. A lack of data also makes cyber-insurance appear less desirable to companies, while simultaneously increasing the price of cyber-insurance.

PUBLIC POLICY STEPS

Given the public policy benefits that come with widespread adoption of cyber-insurance and the current obstacles to the widespread creation and adoption of cyber-insurance, the federal government should act in order to help counteract the current market failure in the cyber-insurance market. The federal government has a number of measures at its disposal that it may use to improve the market for cyber-insurance, and by doing so help shore up domestic and international cyber-security.

FEDERAL PURCHASING POWER

The federal government can promote the use of cyber-insurance with its strong position in the marketplace, by including provisions in government contracts and sub-contracts which hold or are too connected to sensitive government data on cyber-insurance. This would permit the marketplace to immediately judge the quality of the contractor's security systems, require the necessary improvements, if any, to be eligible for insurance benefiting the government as a customer of the contractor and would also directly stimulate the cyber-insurance market by increasing demand for cyber-insurance. Further down the line, companies would be able to use their insurance as a selling point when bidding on private contracts, leading to further uptake of cyber-insurance by their competitors to nullify this advantage.

Precedent for this action may be found in the Federal Acquisition Regulations, which require government contractors "to provide insurance for certain types of perils."

ENCOURAGE INFORMATION-SHARING

The federal government can promote the sharing of cybersecurity information by establishing an antitrust exemption to allow insurers to pool data on vulnerabilities and attacks. This would allow insurers and risk managers to create better actuarial models for cyber-risks, reducing insurance premiums and making cyber-insurance more attractive to companies, and therefore increasing the adoption of cyber-insurance. Precedent for this approach may be found in the Year 2000 Information and Readiness Disclosure Act of 1998, which provides a limited exemption from federal antitrust law and the Freedom of Information Act for the sharing of vulnerability information related to the Year 2000 bug. This action would result in the production of a comprehensive and detailed compilation of cyber-security information at no cost to the taxpayer. By reducing the uncertainties currently associated with cyber-risks, it would tend to drive down the supply cost of cyber-security insurance and reinsurance, leading to lower prices and increased coverage rates. Insurance companies are best placed to compile

this data, and already require policyholders to report cyber-attacks. This action would help to reduce the current under-reporting problem at no cost.

Further the federal government could encourage and support the creation of an insurance information sharing organization similar to the current ISO (Insurance Service Organization) model, the Underwriter's Laboratory model, or the previously discussed SemaTech model.

RECOMMENDATIONS

1.) Include provisions on cyber insurance in government contracts. Doing this would improve cyber-security among government contractors, with a chance that private industry would adopt a similar policies, resulting in high cyber-insurance coverage rates and a corresponding increase in cyber-security generally. The regulatory burden of added by such a requirement would be minimal, and the cost to the taxpayer would most likely be low.

2.) Establish an antitrust exemption to promote the sharing of information and data relating to cyber-security. This actuarial data would allow the risks and benefits of a particular cyber-insurance policy to be calculated more accurately, allowing insurers to charge lower premiums and allowing and making cyber-insurance more attractive to risk managers. There would be no associated cost to the taxpayer.

3.) Consider a measure aimed at reducing the fear of a "cyber-hurricane" among insurers. The two best options for doing so are providing incentives for insurers to establish an ISO or UL model organization to share information, and offering a tax deduction encouraging insurers to increase the capital reserves used to pay out cyber-insurance claims.

• *What other market tools are available to encourage cybersecurity best practices?*

ISA Response

Streamlined Regulation - Nearly every company in the world has by now factored into its business plan the wonders of digitalization----web based marketing, international supply chains, VOIP instead of traditional telecommunications and remote workers. Yet, as described above we are not getting the investment in cyber security that we should.

This is true for the federal government as well. For example the Obama Administration has announced a "cloud first" strategy for the federal electronic systems that they claim will save them between 20-50 billion dollars a year. Some of that money ought to be being plowed back into system wide---not just government or "I3S"---cyber security.

However, assuming that none of this money will be invested in market incentives, there are still many levers the federal government can pull to generate more private cyber investment across industry that require little or no government spending. Ironically, many of these incentive structures are widely used in other areas of our economy; we simply have not yet applied them to cyber security.

The key is to reduce government induced costs on industry, rather than provide direct government subsidies such as with tax incentives.

An example is streamlined regulation, or, as appropriate, accelerated permitting and approvals. For example, many enterprises are buckling under redundant cyber security auditing requirements. If the government could develop a sound baseline audit to simply remove the redundancy, this could be

offered as a carrot to enterprises that demonstrate investment in proven effective cyber security techniques such as those identified in the Verizon/U.S. Secret Service report that has been previously discussed.

On a broader scale there are numerous outdated analogue based laws (see the Administration's "Cyberspace Policy Review," Appendix A) that could be possibly modified to reduce cost to industry.

• *Should federal procurement play any role in creating incentives for the I3S? If so, how? If not, why not?*

ISA Response

While the answer is, "yes," using government procurement incentives should be utilized across industry, not just for "I3S." Government procurement --- and not just for IT equipment---could be tied to more stringent cyber security on the part of firms that compete for government contracts, or access existing (not additional) government spending programs (e.g., small business loans---and all the TARP money should have come with cyber security requirements). In these cases, we are not talking about government spending more, we are simply talking about who gets the spending the government is making---weigh it more heavily in terms of the compelling national interest of cyber security. No new spending is required.

If the procurement practice continues to revolve around lowest cost, and not product assurance, the market will not respond with higher priced high assurance products.

Policy Recommendation B2a:
Congress should enact into law a commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows states to build upon the framework in defined ways. The legislation should track the effective protections that have emerged from state security breach notification laws and policies.

Policy Recommendation B2b:
The Department of Commerce should urge the I3S to voluntarily disclose their cybersecurity plans where such disclosure can be used as a means to increase accountability, and where disclosure of those plans are not already required.

Questions/Areas for Additional Comment:
• How important is the role of disclosure of security practices in protecting the I3S? Will it have a significant financial or operational impact?
• Should an entity's customers, patients, clients, etc. receive information regarding the entity's compliance with certain standards and codes of conduct?
• Would it be more appropriate for some types of companies within the I3S be required to create security plans and disclose them to a government agency or to the public? If so, should such disclosure be limited to where I3S services or functions impact certain areas of the covered critical infrastructure?

ISA Response

Research has shown consistently that the single biggest barrier to enhancing the cyber security of our nation's critical infrastructure is economic. The National Infrastructure Protection Plan (NIPP) 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, and the Cyberspace Policy Review released by the Obama Administration in spring of 2009 specifically advocated the development of market incentives such as procurement, tax and liability to incentivize additional cyber security investments.

These policy commitments have yet to be fulfilled. In fact, the Department of Commerce, and even the recent Administration legislative proposal, rely primarily on "disclosure" as a market incentive to generate increased cyber security investment.

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 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.

"Breaches" were the big cybersecurity concern of the last few years, but they are not the big cybersecurity 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 it. This is a way of thinking about cyber security that many of the foremost cybersecurity experts have been arguing is obsolete for approximately a 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

In fact, most companies are unable to tell whether it has been the victim of a successful cyber attack unless it makes a special effort to investigate, spends additional resources on the effort, and has 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 degree of motivation.

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 investigators, who 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 disclosing such plans would be another, costly level of administrative bureaucracy and auditors that would probably only be getting it the way of good security.

THE INFORMATION GENERATED BY THESE DISCLOSURES WON'T ENHANCE SECURITY

Ironically, one of the more general 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 already 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. 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 this 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.

AN EFFECTIVE REPORTING AND DISCLOSURE SYSTEM CAN BE DEVELOPED

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 further ones. 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 account of 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 be 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.

Policy Recommendation B3:
The Department of Commerce should work with other agencies, organizations, and other relevant entities of the I3S to build and/or improve upon existing public-private partnerships that can help promote information sharing.

Questions/Areas for Additional Comment:
- *What role can the Department of Commerce play in promoting public-private partnerships?*
- *How can public-private partnerships be used to foster better incentives within the I3S?*
- *How can existing public-private partnerships be improved?*

ISA Response

The security of private-sector and government network infrastructure is a national priority. U.S.-based information networks and critical infrastructures are complex and diverse, and most of them are owned and operated by the private sector. Industry has been working continually to enhance the security and resiliency of these systems and is committed to continuing these efforts through a voluntary partnership with government. Industry players have created and developed new products and services that make up information systems and networks, and they continue to innovate to enhance those products and services for operability, productivity, stability and security.

Given the complexity and interconnected nature of information systems and networks, as well as an ever-evolving and sophisticated threat environment, no one organization or entity can address U.S. national cybersecurity alone. Industry players must work together, government entities, such as the Department of Commerce, must harmonize their approaches to protecting the entire cyber ecosystem, government and industry must work together to address common concerns and build collaborative solutions, and government should refrain from creating hard to define classifications such as "I3S". The cybersecurity public-private partnership, particularly with respect to critical infrastructure protection, has an evolutionary history that has culminated in the partnership structure that government and industry collectively created and utilize today under the National Infrastructure Protection Plan (NIPP).[3]

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, "and should be broadened to include all segments of the cyber ecosystem]. 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. Key components of a workable public-private partnership can be heavily derived from the "Cyberspace Policy Review" (CSPR) and industry priorities.

Government and industry sources have documented the substantial progress the current market-oriented process has made. In 2009, President Obama commissioned staff from the National Security Council to conduct an intensive review of our nation's cybersecurity which found that "many technical

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

and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity."[4]

As previously mentioned, the marketplace has seen the development of many products and services that provide for greater cybersecurity. Their effectiveness has been affirmed by both government and industry studies that note that a significant number of cyber events could have been prevented or had their effects mitigated by using the standards practices and technologies the marketplace has already created.[5]

The CSPR's finding that cost and complexity, not lack of ability or commitment, are the largest problems in implementing effective cyber solutions has also been confirmed by multiple independent studies. 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.[6] As President Obama has noted, "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."[7]

A number of policy and operational accomplishments have already been achieved through current industry-government partnership. These accomplishments include the development of cybersecurity standards and best practices through the global, multi-stakeholder ecosystem of standard-setting organizations, creation of the Sector Coordinating Councils, Critical Infrastructure Partnership Advisory Council (CIPAC) legal structure, the completion of a National Cyber Incident Response Plan (NCIRP), the successful execution of the Cyber Storm exercises, and several sector risk assessments. There have also been improvements in information-sharing mechanisms, such as Information Sharing and Analysis Centers (ISACs), the National Council of ISACs and other successful sector-specific information-sharing mechanisms, and the launch of the National Cybersecurity and Communications Integration Center (NCCIC), with seats designated for government and industry enabling ongoing coordination, planning and response.

While all these efforts and others make government and industry more coordinated and secure, the partnership has not yet been utilized to implement the economic, technical and operational issues the NIPP calls for. The CSPR confirms this observation:

---

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

[5] Aerospace Industries Association Annual Conference, *Robert Bigman comments on Cyber Security,* Washington, DC in October 2008; U.S. Senate, hearing before the Committee on Judiciary, Subcommittee on Terrorism and Homeland Security, *Testimony of Richard C. Schaffer, Jr. Information Assurance Director of the National Security Agency,* November 17, 2009, http://judiciary.senate.gov/pdf/11-17-09%20Schaeffer%20Testimony.pdf, Verizon, *2010 Data Breach Investigations Report,* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf; PricewaterhouseCoopers, *The Global State of Information Security*, 2005; Verizon, *2008 Data Breach Investigations Report, http://www.verizonbusiness.com/resources/security/databreachreport.pdf.*

[6] 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.

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

> "The public-private partnership for cybersecurity must evolve to define clearly the nature of the relationship including the roles and responsibilities of each of the partners."[8]

The partnership structure that industry and government collectively created under the NIPP clearly articulates what is required to build this system. Government and industry have the opportunity to work more collaboratively to implement the following agreed upon activities:

> "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). 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."[9]

The public private partnership is the right model but it needs to be evolved to meet the modern threats and more fully implemented---especially by the government partners. The missing link in this partnership, however, has been the lack of incentives, a position the ISA has stated since the first publication of the National Strategy to Secure Cyber Space (2002).

Again, research has long demonstrated that that only a substantial minority (probably between 30% and 40%) of enterprises have what may be called a natural ROI for security investment. When such as natural confluence occurs then private sector entities will make [in] adequate security investment.

For most of the private sector, security is simply an economic consideration. If you own a warehouse and 10% of your inventory is "walking out the backdoor" every month, you will not buy the cameras hire the guards etc. to solve your security problem if your study shows that it costs 11% to do so. That is a good risk management decision from a private sector perspective.

The public sector has economic considerations, but also additional non-economic considerations (national security, privacy, politics etc.) and thus may have a lower risk tolerance than their private partners because they simply assess risk differently.

---

[8] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure,* May 2009 at 33.

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

However, as the trade associations who signed onto that paper have attested, we recognize that in an interconnected cyber world the private sector may be required to take on new, non-economic and traditional public sector responsibilities with respect to cyber security.

Therefore the public private partnership which has heretofore ignored the economic aspects of cyber security needs to evolve into a fuller and more sustainable model which includes government finding ways to offset the non-economic investments it would like private industry to make in the interests of broad national security.

Accordingly, a new policy initiative by the Department of Commerce or other department or agency that seeks to replace or modify the current public-private partnership model with an alternate system more reliant on government mandates directed at the private sector is of concern. Such a change of direction would both undermine the progress that has been made and hinder efforts to achieve lasting success. Rather, the Department of Commerce and the government as a whole should build on and off of the promise and progress articulated by the NIPP and the CSPR. In sum, the Department of Commerce should work within the public-private partnerships that have already been established and heed the pledge President Obama made upon the release of the Administration's CSPR: "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."

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 can only be achieved through a true partnership between the public and private sectors.

• What are the barriers to information sharing between the I3S and government agencies with cybersecurity authorities and among I3S entities? How can they be overcome?
• Do current liability structures create a disincentive to participate in information sharing or other best practice efforts?

ISA Response
In the Cyberspace Policy Review, the Administration articulated the barriers to information sharing as follows:

"Some members of the private sector continue to express concern that certain federal laws might impede full collaborative partnerships and operational information sharing between the private sector and government. For example, some in industry are concerned that the information sharing and collective planning that occurs among members of the same sector under existing partnership models might be viewed as "collusive" or contrary to laws forbidding restraints on trade. Industry has also expressed reservations about disclosing to the Federal government sensitive or proprietary business information, such as vulnerabilities and data or network breaches. This concern has persisted notwithstanding the protections afforded by statutes such as the Trade Secrets Act and the Critical Infrastructure Information Act, which was enacted specifically to address industry concerns with respect to the Freedom of Information Act (FOIA). Beyond these issues, industry may still have concerns about reputational harm, liability, or regulatory consequences of sharing information….

"… In addition, the challenges of information sharing can be further complicated by the global nature of the information and communications marketplace. When members of industry operating in the United States are foreign-owned, mandatory information sharing, or exclusion of such companies from information sharing regimes, can present trade implications."[10]

To overcome these barriers, the ISA has suggested an alternative approach to information sharing, which is described above as the Command and Control Disruption Strategy

[10] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 18-19

Policy Recommendation C1:
The Department of Commerce should work across government and with the private sector to build a stronger understanding (at both the firm and at the macro-economic level) of the costs of cyber threats and the benefits of greater security to the I3S.

Questions/Areas for Additional Comment:
• What is the best means to promote research on cost/benefit analyses for I3S security?
• Are there any examples of new research on cost/benefit analyses of I3S security? In particular, has any of this research significantly changed the understanding of cybersecurity and cybersecurity related decision-making?
• What information is needed to build better cost/benefit analyses

ISA Response

THERE IS NOT NECESSARILY A DIRECT ALIGNMENT BETWEEN INCIDENTS AND PERCEIVED NEED TO MAKE CYBER SECURITY INVESTMENTS

One of the most common, and simplistic, assumptions made is that if the impact of cyber incidents are severe, than it will naturally follow that adequate investments to stop the attacks. A corollary to this belief is that bad behavior, including inadequate security investments by private corporations will naturally be sanctioned economically and this economic penalty will provide a check on poor cyber security practices.

Such assumptions seem to underlie the above recommendation and questions and betray a misunderstanding of the unique characteristics of cyber security.

As noted before, in the world of cyber security, it is not necessarily the entity that is negligent or culpable that receives the economic penalty for that behavior. Anderson and Moore's review of the literature of information security came to precisely this conclusion noting that "Legal theorists have long known that liability should be assigned to the part that can best manage the risk. Yet everywhere we look we see online risk allocated poorly…people who connect insecure machines to the Internet do not bear the full consequences of their actions …(and) developers are not compensated for costly efforts to strengthen their code"[11]

By illustration consider the case of a poor cyber citizen who does not practice good cyber hygiene. He visits suspect web sites, downloads and opens unfamiliar e-mail and attachments and uses obvious and common passwords which he never alters. Not surprisingly, this person will find their identity stolen.

The thief naturally runs up thousands of dollars in fraudulent charges on our hero's credit cards. Who is responsible for this unfortunate incident and who suffers the economic consequences?

Our sloppy cyber hero will suffer minimal economic damages. The economic damages created by this "bad actor" will in fact be visited upon the bank which holds this individual's credit card which actually bears little or no real culpability for the harms that occur. Moreover, as McCarthy noted in his 2010 study "Retail payment systems exhibit a kind of technical externality. Damage is not contained at one node of the payment network but affects other nodes. Cardholder information might be obtained at one merchant location and used for card fraud at other merchants. In this way, security vulnerabilities in one

[11] R. Anderson and T. Moore, *The Economics of Information Security*. In journal *Science* 314 (2006).

part of the payment system merchant or processor location potentially affect merchants, cardholders and financial institutions in other parts of the system."[12]

The argument here is not that this sort of consumer protection system is bad or inappropriate. Rather, the argument is that the economic impacts are not correlated with the bad behavior. As a result a measurement system that seeks to properly gage the impacts of cyber attacks must take into account this counterintuitive reality.

A similar complication occurs when considering corporate security issues associated with the theft of intellectual property. An economic model developed by Kunreuther and Heal notes that security investments can be strategic complements: An individual taking protective measures creates positive externalities for others that in turn may discourage their own investments.[13] Bhum and Katarina termed this the problem of "interdependent risk" in which a firm's IT infrastructure is connected to other entities, so that its efforts may be undermined by failures elsewhere.[14] This correlated risk makes firms under invest in both security technology and cyber insurance, which will be discussed in greater detail in Question 8. Finally Anderson and Moore survey of the literature on information security puts it succinctly "Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail."[15]

As an example, assume a criminal or rogue state entity may desire to steal intellectual property from a high value target. Accessing the target directly may be difficult because the target organization has made substantial investments to prevent unauthorized traffic from entering its system.

However, since the Internet is characterized by broad interconnectedness the target entity may in fact be connected with other entities which have not made substantial investments. The criminal or rogue entity may attack this weaker element in the system and through that window gain access to the ultimate target.

In this instance, which may describe many attacks in the defense industrial base, the point of the attack and the target of the attack may be entirely different entities. Further, the edge entity that is the point of the attack may not be suffering any economic impact from the attack and thus from this entity's perspective the attack may not be considered a significant incident. Moreover, this entity has little incentive to prevent similar attacks.

On the other hand the ultimate target not only suffers potentially severe impacts notwithstanding its defensive investments---but finds that these investments are in fact being undermined by the entity on the edge which is the point of the attack.

Finally, as suggested above, governments often operate on entirely different economic basis than private entities. Consider the economics of cyber weaponry, for example within the context of compromised supply chains. It's well known that information technology supply chains are usually international in composition and thus highly subject to compromise either via software or hardware compromises.

---

[12] MacCarthy, Mark, *Information Security Policy in the U.S. Retail Payments Industry,* June 2010
[13] H. Kunreuther and G. Heal, *Interdependent Security*. In journal of *Risk and Uncertainty* 26, 231 (2003).
[14] A. Arora, R. Krishnan, A. Nandkumar, R. Telang and Y. Yang, *Impact of Vulnerability Disclosure and Patch Availability – An Empirical Analysis*, Third Workshop on the Economics of Information Security (May 2004, Minneapolis, MN)
[15] R. Anderson and T. Moore, *The Economics of Information Security: A Survey and Open Questions*

Attacks on the hardware of military IT supply chains can be especially devastating since once completed the malware may be virtually undetectable until it is activated, which may not come until the weapons system is launched. At that time the malware could be capable of misfiring the weapon system or even having it turn back on the entity that launched it in the first place.

The good news is that this type of hardware based IT supply chain attack is fairly difficult to do and prohibitively expensive in most cases. In fact, most criminal entities would be far more likely to engage in less expensive, and more resilient, software supply chain attacks to achieve their economic gains.

However, since nation states operate on very different economic assumptions than corporate entities they may be willing to spend exorbitant amounts of money on a single use weapon---as was the case with hundreds of billions of dollars invested for decades to build nuclear weapon arsenals never intended for us. In fact some economist blame this phenomenon as the reason that economists have recently abandoned the study of security. Mastanduno noted that the key reason for the general absence of economic analysis of security issues was that nuclear weapons had basically decoupled national survival from economic power.[16]

Compared to this historic pattern of government investment the sort of investment needed to inserted malware in the hardware of a weapon system supply chain ---that would be uneconomic even form most criminal organizations---becomes economically very reasonable.

Private entities engaged in a risk management approach to managing their own cyber security might find little economic payoff in preventing these hardware supply chain attacks since they are unlikely to affect their own bottom line. Conversely governments may have an extremely high need for vigilance in this area.
In this dramatic instance the government's unique cyber problems are not equally shared by the privet entities that make up the bulk of the supply chain.

As such, analyzing and measuring the impacts of cyber events and the necessary investments to address them is complicated by the differing economics affecting government and industry. Any model developed to measure the effects of events and the required investments to prevent them must affirmatively account for these variables.

[16] M. Mastanduno, *Economics and Security in Statecraft and Scholarship*, International Organization, v 52, no 4 (Autumn 1998)

Policy Recommendation C2:
The Department of Commerce should support improving online security by working with partners to promote the creation and adoption of formal cybersecurity-oriented curricula in schools. The Department of Commerce should also continue to increase involvement with the private sector to facilitate cybersecurity education and research.

Questions/Areas for Additional Comment:
• What new or increased efforts should the Department of Commerce undertake to facilitate cybersecurity education?
• What are the specific areas on which education and research should focus?
• What is the best way to engage stakeholders in public/private partnerships that facilitate cybersecurity education and research?

ISA Response

While much attention has rightfully focused on educating consumers and youth, an educational effort aimed at building awareness among business owners, managers, and employees that cybersecurity is an enterprise risk management issue needs to be further developed and communicated through the partnership. A view of cybersecurity solely as an IT problem masks the larger financial risks cyber vulnerabilities hold for the entire enterprise and could result in under-investing in cybersecurity. However, businesses can substantially reduce the negative consequences of a successful cyber incident through risk management across the entire organization. Promotion of ongoing employee evaluations regarding cybersecurity awareness and cybersecurity policy compliance is needed.

The interconnectedness of computers and networks in cyberspace means that the public and private sectors share responsibility for promoting security as an enterprise-level objective. The CSPR captures this point succinctly: "It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts.

Again, while the development of school curricula is laudable; it suggests an excessively narrow view of the cyber security problems we face.

PricewaterhouseCoopers conducts the largest corporate information security survey in the world. Their 2008 study concluded:

> *"The security discipline has so far been skewed toward technology—firewalls, ID management, intrusion detection—instead of risk analysis and proactive intelligence gathering. Security investment must shift from the technology-heavy, tactical operation it has been to date to an intelligence-centric, risk analysis and mitigation philosophy... We have to start addressing the human element of information security, not just the technological one, it's only then that companies will stop being punching bags."*[17]

"Cyber Space Policy Review" released by the President in May of 2009 makes this same point.

> *"It is not enough for the information technology workforce to understand the importance of cyber security; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and*

[17] PricewaterhouseCooper, *The Global State of Information Security*, 2008

potential impacts. If the risks and consequences can be assigned monetary value, organizations will have greater ability and incentive to address cyber security. In particular, the private sector often seeks a business case to justify the resource expenditures needed for integrating information and communications system security into corporate risk management and for engaging partnerships to mitigate collective risk."[18]

Unfortunately, American enterprises are not properly assessing their financial cyber risk and as a result are not making the investment decisions the Cyber Space Policy Review suggests are needed to create and maintain a resilient system of cyber security.

Despite an avalanche of data indicating that cyber vulnerabilities, attacks and loses are mounting at an increasing pace, two recent large scale studies have shown that American companies are actually---and sometimes dramatically-- reducing their investment in cyber security.

PricewaterhouseCoopers 2009 survey reveals that, nearly half (47%) of all the enterprises studied reported that they are actually reducing or deferring their budgets for information security initiatives, even though a majority of respondents acknowledged that these cost reductions would make adequate security more difficult to achieve.[19]

These results are confirmed by a separate large scale study conducted by the Center for Strategic and International Studies released in 2010 which reported that between 2/3 of IT budgets had been reduced often by 15% or more and cuts were even more significant in critical sectors such as Energy, oil and gas where up to 75% reported reductions.

The CSIS study concluded that "overall cost was the most frequently cited as the biggest obstacle to ensuring security of critical systems followed by lack of awareness." The study also commented "The number one barrier is the security folks haven't been able to communicate the urgency well enough and they haven't been able to persuade the decision makers of the reality of the threat."[20]

The fact is that American businesses are primarily thinking of cyber security as an "IT" problem rather than appreciating it as the enterprise-wide risk management issue that it really is… Moreover there are structural barriers impeding the necessary communication between the IT specialists and the rest of the organization---most notably the senior executives responsible for investment decisions.

Deloitte's 2008 "Enterprise Risk" study concluded that, in 95% of US companies, the CFO is not directly involved in the management of information security risks, and that 75% of US companies do not have a Chief Risk Officer.[21]

---

[18] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009.
[19] PricewaterhouseCoopers, *Trial by Fire*, 2009.
[20] Center for Strategic & International Studies, In *the Crossfie: Critical Infrastructure in the Age of Cyber War*, 2009.
[21] Deloitte, *Information Security & Enterprise Risk 2008*, Presentation to CyLab Partners Conference, Carnegie Mellon University, Pittsburg, PA, October 15, 2009.

The Deloitte study went on to document that 65% of US companies have neither a documented process through which to assess cyber risk, or a person in charge of the assessment process currently in place (which, functionally, translates into having no plan for cyber risk at all).[22]

The Carnegie Mellon University (CMU) CyLab 2010 Governance of Enterprise Security Study concluded: "There is still a gap between IT and enterprise risk management. Survey results confirm that Boards and senior executives are not adequately involved in key areas related to the governance of enterprise security."[23]

The 2008 CMU study also provided alarming details about the state and structure of enterprise risk management of cyber security.[24] The study pointed out that:

- 83% of corporations do not have a cross-organizational privacy/security team.
- Less than half of the respondents (47%) had a formal enterprise risk management plan.
- In the 1/3 of the 47% that did have a risk management plan, IT-related risks were not included in the plan.

The Internet Security Alliance and the American National Standards Institute have developed a model to address this problem. The ISA-ANSI project involved more than 60 private entities and 13 government agencies over a two year period. The results were two publications ("50 Questions Every CFO Should Ask About Cyber Security" and the Financial Management of Cyber Risk").

These publications provide a detailed framework that reviews cyber security on an enterprise wide basis analyzing cyber issues from the unique perspectives of the human resource manager, the operations team, the legal and compliance offices, as well as the risk management and communications operations. The framework provides a mechanism to better analyze the financial aspect of the issue in a way that can be better understood, managed and invested in by the CFO or other senior executives.

An educational program built on this framework and targeted to senior executives would yield a better understanding of cyber threats and solutions in enterprises. Moreover the "trickle-down" effects on employees throughout the organization, many of whom will take home these lessons to their children could jump start a nationwide enhancement of cyber security.

---

[22] Deloitte, *Information Security & Enterprise Risk 2008*, Presentation to CyLab Partners Conference, Carnegie Mellon University, Pittsburg, PA, October 15, 2009.
[23] Carnegie Mellon CyLab, *Governance of Enterprise Security Study: CyLab 2010 Report*, June 2010
[24] Carnegie Mellon: CyLab, *Governance of Enterprise Security Study:CyLab 2008 Report*, December 2008

Policy Recommendation C3:
Through its continued research efforts, the Department of Commerce should begin to specifically promote research and development of technologies that help protect I3S from cyber threats.
Questions/Areas for Additional Comment:

• What areas of research are most crucial for the I3S? In particular, what R&D efforts could be used to help the supply chain for I3S and for small and medium-sized businesses?

ISA Response

There are several cyber security disciplines/technologies that would benefit from increased funding

i. Systems availability: A means for automated hot recovery preserving availability (no cold restarting).
ii. Configuration management and control: real time configuration assessments (ability to perform scans and vulnerability assessments at line speeds as opposed to off-line speeds.).
iii. Agile defenses that change profile, from an attacker point of view, and provide line speed sensing and queuing (that includes reducing the information density and load), and cyber situational awareness.
iv. Cohesive data protection strategies for data at rest, in motion, and in use. Many suppliers provide solutions today to address encryption of disks and transports but do not have mature solutions for managing the information lifecycle through content discovery, consistent and effective labeling, and then the application of appropriate protection policies based on the resulting content categorization. The inability to protect the actual content at the right levels forces many organizations to protect entire networks, servers, and disks (fixed and portable), which is very inefficient and may create barriers to effective monitoring within their computing environment with such a high percentage of the traffic being encrypted.
v. Cyber Risk Mitigation Metrics– Today's methods and techniques for mitigating risk associated with protection of sensitive data lack clarity as to a risk reduction value for application of a specific countermeasure to a particular designed architecture that may be determined to have a specific weakness. These metrics would be helpful in making business decisions as to which countermeasure should be applied to adequately strengthen data protection. For example, the decision of adding a firewall or improving the strength of authentication to an application housing sensitive intellectual property would be simplified if a risk reduction value could be weighed against the cost to implement either.
vi. Massive Information Management and Data Analytics - The development of applications that rely on databases containing petabytes of information is driving the need for improved information management. Issues surrounding data uncertainty, structured queries and protection profiles of large data sets need to be addressed as the complexity and volume of information repositories rapidly grow.
vii. Advanced Persistent Threat (APT) concerns– With the advancement in level of sophistication of our adversaries' capabilities and techniques, our abilities in prevention, detection and correction have lagged the adversarial growth and sophistication. New techniques in covert channel and data infiltration detection must be developed so that incident response teams can react more quickly on reliably detected events. Further, our ability to reestablish compromised systems as trusted systems on the network at near real time must be developed. The ability to "play through" and continue the mission when under attack will be a critical success factor for many public cloud-based offerings

• *What role does the move to cloud-based services have on education and research efforts in the I3S?*

ISA Response
See APT response above

• *What is needed to help inform I3S in the face of a particular cyber threat? Does the I3S need its own "fire department services" to help address particular problems, respond to threats and promote prevention or do enough such bodies already exist?*

ISA Response
No, a Department of Commerce "Fire Department" is not necessary. What's necessary is one "fire department" that all companies across the cyber ecosystem can call for cyber assistance.

As we explained in our multi-association White Paper:
"Companies and government entities regularly and successfully respond to cyber attacks and other intrusions on their networks. In many organizations, there are processes and procedures for incident response and reporting that are used to protect their networks and information assets on a regular basis. It is when an incident becomes too big or complex for one organization to handle alone that collaborative incident management – and partnership – is important in order to prevent, defend against, and recover from the attack. Many attacks have called for collaborative action, and public and private partners learn from each incident how to communicate, share information, and remediate the problem. In addition, they engage in exercises that are designed to test processes and plan for incident response from which they continue to learn what the most effect measures are in any given circumstance.

The Cyber Storm exercise series has been an excellent tool for understanding the possible course of any particular incident – or combination of attacks – and for assessing existing response measures and determining gaps. Industry has been a partner in the planning and play of the exercises, which have spanned the critical infrastructure sectors and incorporated many aspects of attacks on that infrastructure. In each of the three Cyber Storm exercises, the participants have used the lessons learned to make corresponding changes in their internal procedures and in the procedures used to collaborate among the participants.

In the most recent Cyber Storm III exercise, the scenarios tested the preparation and processes laid out in the National Cyber Incident Response Plan (NCIRP) completed prior to the exercise. The development of the NCIRP was a collaborative process between industry and government. It resulted in a plan that was meant to be instructive for both groups, but flexible enough to accommodate the varying types of scenarios that could occur. The official results and lessons learned from Cyber Storm III are still being assessed and reported, but the immediate observations from the exercise are already being evaluated and integrated into organizations' planning procedures.

Rigid response protocols and procedures are not effective in managing each possible type of incident, and it has been important to recognize and acknowledge that there is no one-size-fits-all in cyber incident response. Cyber incidents do not occur in one moment; they can evolve and grow in nature and impact over time. These attributes require flexibility and an iterative evaluation mechanism that includes impacted parties – those that are the victim(s), and those that can provide assistance. In that

vein, it is important to have an ongoing, sustained collaboration mechanism to continuously assess the problem as it occurs over time and to determine the most effective response tools.

Through the National Cyber Coordination and Integration Center (NCCIC), government and industry are in the early stages of implementing a long-standing recommendation that industry responders from the IT and communications sectors should work together with their government counterparts in an integrated operations center so that their respective expertise, analysis, and response capabilities can be shared and leveraged on a sustained basis – not just in times of crisis. The NCCIC is a very positive development in the public-private partnership and should be strengthened by the full participation of industry.

Government should fully establish industry's seat in the integrated watch center and begin evaluation and process for growing industry's presence; industry should ensure a long-term plan for filling the watch center seats; and participants should report lessons learned from collaborative exercises as soon as possible and undertake improvement measures on a timely basis."

• *What role should Department of Commerce play in promoting greater R&D that would go above and beyond current efforts aimed at research, development, and standards?*

ISA Response

We should begin by noting that a critical area for the government to focus on is R&D for innovation.

The broad issue of cyber innovation encompasses more than just the R&D issues raised in this inquiry including authentication/identity management, website/component security, and perhaps even product assurance, however we will address these issues under this more general question.

Innovation and the need and requirements for developing and instituting an approach to promoting innovation, are relevant to each of the major problem areas in cybersecurity, and the development and evolution of information technology, generally. As suggested in the Federal Register notice, promoting innovation is critical to the long-term economic and security posture of the nation. If innovation only encourages R&D and does not facilitate information sharing about exciting new technologies, practices and awareness/training, it will only address part of the long-term challenge.

Given the role of the Commerce department in cyber R&D, and its broader interest in innovation, generally, Commerce should consider developing or at least supporting the development of an information-sharing and collaboration architecture and process to promote cyber innovation in both the CI/KR and non-CIKR areas, and with and across government. There is no system or process in place in the U.S. to facilitate that kind of information sharing across government, much less with the private sector and academia, about cyber security requirements and what technologies contribute most effectively to meeting those (or new) requirements, and where R&D or other development (standards, practices, etc.) is necessary to fill the gaps.

Launching such a capability will help inform government, the private sector, and academia of what the current set of cybersecurity requirements is in particular problem areas (such as identity management, asset discovery, secure web transactions, risk management, vulnerability detection, etc.), whether and to what extent current technologies exist that can meet those requirements (and/or inform the need for additional requirements). This can be a totally voluntary system that can be used by government

agencies to inform RFI's and RFP's, and let them know of the existence of cutting-edge technology roadmaps, and inform government R&D.

Part of the problem we face on the innovation front is a failure to recognize that while isolated efforts at innovation are a good thing, we need to make it easier to share information about and leverage the benefits of innovation. In addition to facilitating information sharing about requirements and experience with trying different technologies to address those requirements, it is important to systematize a process that allows and encourages companies – even small and new ones – to provide input on how their technology(ies) can meet the identified requirements. Not just in a Garnter-magic quadrant level of granularity, but with actual specifications on what the respective technology can deliver.

An architecture and process such as envisioned here will actively facilitate and encourage those who buy technologies (or invest in or test technologies) to consider a much wider range of technologies. It will also encourage companies who want to improve their competitiveness to see what the specifications are among their competitors and strive to improve their technologies or develop new ones. Where there are gaps in currently available technologies, the availability of information through this process can inform R&D spending and it can encourage government and the private sector to partner with one or more smaller companies' whose technologies show real promise to engage in a collaborative technology roadmap.

More specifically, corporate IR&D decisions align to technologies and capabilities expected by the corporation to be needed by the customer. This customer expectation is often gauged by direct interaction with the customer at the agency level. The scope of this interaction can be limited to silo'ed needs and is likely focused on short term needs of the agency without regard to coincidental needs of other agencies. Therefore a consolidated, well known and integrated strategy and roadmap for mission needs and support would enable corporations and sponsors to make better informed decisions on spend corporately and will help to ensure that the overall portfolio of IR&D investments are coordinated and well-aligned to meet research objectives.

i. For IR&Ds that are past the proof of concept stage (higher technology readiness levels or TRLs): One way is to use the United Kingdom engagement model derived from the Technology Strategy Board (TSB). The TSB sponsors programs that provide matching funding to promote the development and commercialization of concepts that have commercial viability. Proposals for this funding must have a business plan and a mechanism for executing that plan. Teams are composed of academic and commercial entities performing cooperative research leading to commercial product development.
ii. For more strategic or lower TRL, budget priorities usually adversely affect long range research so an increase in longer range research that develops industry-academia partnerships would be desirable. These partnerships work together to design and create solutions that provide the next generation of protection while distributing the innovation and the development risk.

The disciplines that require the most research and development resources are in the areas of analytics to provide faster, more robust detective controls. And standards development to facilitate automated control evaluation and management for multi-vendor, dispersed, and diffused applications (e.g. VoIP service).

Finally, the insurance industry potentially has an important role to play here. Providing R&D funds to a to be created insurance information sharing organization similar to ISO (insurance organization services) to fund frequency and severity of losses could prompt more insurers to provide cyber insurance as well as create defacto best practices and agreed upon loss statistics.

Policy Recommendation D1:
The U.S. government should continue and increase its international collaboration and cooperation activities to promote cybersecurity policies and standards, research and other efforts that are consistent with and/or influence and improve global norms and practices.

Questions/Areas for Additional Comment:
• How can the Department of Commerce work with other federal agencies to better cooperate, coordinate, and promote adoption and development of cybersecurity standards and policy internationally?

ISA Response

As described above, there are already adequate best practices and standards being developed to provide substantial safeguards to information systems. The US government via various entities already play's an active role in their development and should maintain that participation.

However, with possible specialized exceptions for unique systems, the US ought not seek to develop their own standards for use by "American" companies.

In an inherently international economy, a set of "US standards' could create a counterproductive response.

The US government ought to devote their resources to funding the analysis and evaluation of the standards created in the market and the provide incentives for enterprises to implement them as described herein.