The Internet Security Alliance (ISA)

Response to the

March 28, 2013 Notice of Inquiry
of the
U.S. Department of Commerce, National Telecommunications & Information Administration

April 29, 2013

Contact:
Larry Clinton, Internet Security Alliance (ISA) President & CEO
Phone: (703) 907-7090
Email: lclinton@isalliance.org
Web: www.isalliance.org

About the Internet Security Alliance (ISA):
ISA is a multi-sector trade association with membership from virtually every one of the designated critical industry sectors, including substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries. ISA focuses exclusively on cybersecurity and cybersecurity related issues as is embodied in its mission, which is to create a sustainable system of cybersecurity by combining advanced technology with economics and public policy.

Founded in 2000 in collaboration with Carnegie Mellon, ISA is also unique in that combines the thought leadership that might be found in a "think tank," with advocacy one would expect from a trade association, and operational security programs that might be found in a professional association.

ISA Board of Directors:
For a current list of the ISA Board of Directors, please refer to Appendix X: ISA Board of Directors, which has been submitted along with the ISA's Response and Appendices to the U.S. Department of Commerce, National Telecommunications & Information Administration's Notice of Inquiry.

Appendices:
The following Appendices will be separately submitted and are to be considered

incorporated hereafter:

- Appendix A: Internet Security Alliance (ISA) Board of Directors List;
- Appendix B: Adaptation of Other Incentives Models to Cybersecurity;
- Appendix C: General Principles Regarding the Use of Incentives in the President's Executive Order; and
- Appendix D: "A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels," by ISA Board Member Jeffrey Brown (Raytheon)"

* * * * *

ISA Response

1. <u>Are existing incentives adequate to address the current risk environment for your sector/company?</u>

A. Which Cyber Risk Are We Talking About?

One of the consensus principles regarding cyber security is that it needs to be undertaken within a risk management framework. Not only is it impractical to simultaneously address all cyber risks, but attempting to do so will spread resources so thinly that all defenses may be weakened, thus, actually undermining security. Unfortunately, there is a lack of clarity regarding precisely which cyber risks are being referenced in the Executive Order (EO), or the present NOI, which emanated as a method to implement the Executive Order in particular.

For example, the EO speaks at several points to catastrophic cyber events and never mentions other threats, such as the theft of intellectual property, personal data or business processes. Meanwhile the National Intelligence estimate released just weeks after the EO indicated that that the likelihood of the sort of catastrophic events alluded to in the EO was currently, and for the next few years, "remote."[1]

Ironically, the main reason why such attacks are considered remote, according to the current Intelligence estimate, is not because they are technologically infeasible but because there seems to be little incentive for those with the capability to launch such attacks to actually do so.[2] The far more common cyber threat – and greatest current

[1] Clapper, James R. Statement to the House Permanent Select Committee on Intelligence. "Worldwide Threat Assessment of the U.S. Intelligence Community." Hearing. April 11, 2013. Web. <http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20WWTA%20US%20IC%20SFR%20%20HPSCI%2011%20Apr%202013.pdf>.

[2] Ibid.

risk – the theft of property, identity and process, is never mentioned in the EO.

The need for clarification along these lines is critical for many reasons, including the fact that defenses for stopping or mitigating attacks focused on theft are, in many instances, fundamentally different than those focused on preventing disruption or destruction. For example, a cyber attack motivated by theft is not successful merely when the attacker breaches a network perimeter. Indeed, this is but the preliminary stage of such an attack. Once in the system, this attacker must also find the target data and then exfiltrate the data successfully from the network, usually to a website or URL.

One of the more successful strategies to mitigate this type of attack is to do sophisticated, often expensive, internal network analysis geared to finding outbound traffic going to unauthorized sites. Once the unauthorized traffic is discovered, the host entity can successfully mitigate the attack simply by blocking the outbound traffic, notwithstanding the fact that the intruder has successfully "breached" the system.[3]

However, this sophisticated strategy may have extremely limited utility against an attacker who has no intention of removing data from the system, but, rather, disrupting or destroying the data or host infrastructure --- the sort of event that may lead to the catastrophic event cited in the EO.

So while it is true that there are some hygienic practices that are generally beneficial against many cyber attacks, it is not true that those practices and standards are going to be as successful in preventing or mitigating sophisticated attacks.

Moreover, we should not take too much false comfort in the oft-reported finding that many attackers are successful using fairly simple attack methods. That finding may well be true. However, it is also true that sophisticated attackers (and the bar on what constitutes "sophistication" is increasingly lowered with diffusion of advanced attack methods throughout the attacker community) will generally use the least costly means to initiate an attack and will upgrade their methods when they meet resistance, such as from the adoption of good standards and practices.

So, while it may well be true that a post facto analysis may indicate that many past attacks could have been prevented with adoption of standards and practices, it is not necessarily true that future attacks (or even these past attacks) would necessarily have

---

[3] Brown, Jeffrey. "A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels." Internet Security Alliance. 2009. Web. <http://isalliance.org/publications/7.%20ISA%20Model%20for%20Disrupting%20Attacker%20Command%20and%20Control%20Channels%20-%20Jeff%20Brown%20(Raytheon).pdf>.

Note – the above cited white paper is also ISA's Appendix D: "A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels," by ISA Board Member Jeffrey Brown (Raytheon)"

been stopped had these standards and practices been deployed, since attackers may well have upgraded the attacks in the face of resistance.

To use a sports metaphor, good pitchers do not use their "best stuff" to strike out weak hitters. If you "show" that you can hit a 90 MPH fastball, a good pitcher will bring you the 92, the 93, or 95 MPH fastball. The attackers posing the greatest risk to our infrastructure are the really good pitchers.

As will be discussed in greater detail below, companies do have incentives to invest in cyber security to address their perceived commercial risk based on a cost-benefit analysis. However, the risks posed by the EO suggest security well beyond that of commercial economics and reach the higher levels of national security. To fully answer the question, the evolving nature of the cyber threat and the level of risk sought and the precise nature of the risks being considered must be clarified.

B. Cyber Defense Is More About Adequate Incentives Than About Technology.

This question about the adequacy of current incentives raises the most fundamental issue in building a sustainable system of cyber security.

In their classic work on the subject, Anderson and Moore noted that misplaced incentives are far more problematic than technology in causing our cyber security problem:

> *"Security failure is caused at least as often by bad incentives as by bad technological design…*Everywhere we look we see online risk allocated poorly…People who connect their machines to risky places do not bear full consequences of their actions. And developers are not compensated for costly efforts to strengthen their code.*"*[4]

The criticality of the incentives issue is even more central to the present exercise revolving around the EO. The centerpiece of the EO is the creation of the NIST voluntary framework for cyber security.

If the framework simply mirrors what our critical infrastructures are already doing, then it is arguably unnecessary, and even potentially harmful, as it could become a ceiling for appropriate behavior.

If, on the other hand, the framework is substantively progressive and voluntary then the only way to generate the behavior described in the framework is either through incentives, off loading cost on consumers or tax-payers, or reducing the attractiveness

[4] Anderson, Ross, and Tyler Moore. "The Economics of Information Security: A Survey and Open Questions." Science 314. 27 Oct. 2006.

of investing in critical infrastructure. There is no free lunch. Of these options, incentives are probably the most attractive.

Moreover, if the incentives are powerful enough, they will generate ongoing improvements in cyber security behavior, and, thus, become more vital to the maintenance of a sustainably secure cyber system than the framework itself.

ISA has outlined 5 criteria of what constitutes an effective incentive:

- In order to be effective, incentives must be powerful enough to effect corporate investment behavior;
- In order to be effective, incentives must be calibrated to at least match the level of additional investment required to adopt the framework proposed under the EO;
- Effective incentives will vary from sector to sector (indeed business to business within sectors) and thus a menu of incentives is needed ---one size does not fit all;
- Regulation that does not include full cost recovery is not a substitute for incentives;
- Costs incurred to increase cyber security, and not compensated from incentives, will invariably come from consumers/tax-payers paying more or through reduced attractiveness in critical infrastructure investment - there is "no free lunch."

C. Right Now the Incentives Favor the Attackers.

The existing imbalance in cyber security incentives is brought into sharp relief when one simply considers the relative incentives that attackers and defenders possess. In the cyber security world, the incentives massively favor the attacking community.

Cyber attacks are currently easy to obtain (they can be accessed for *de minimus* cost, and, sometimes, at no cost) on the Internet. Even highly sophisticated attacks (the so-called "Advanced Persistent Threat" or "APT") are still relatively cheap in relation to the profitability of successful attacks. The "business model" for the attacking community is excellent, as they are able to use the same resources over and over on an unlimited set of profitable targets. In addition, attacks are comparatively easy to launch. Indeed, the attacking can be outsourced and the profits to be generated are enormous, with estimates ranging from the billions to the a trillion dollars in lost revenue as cited in President Obama's "Cyberspace Policy Review."[5]

[5] Executive Office of the President. "Cyberspace Policy Review." 2009. Web. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

Consider then the defender side of the equation: Defenders are almost always a generation behind the attackers, they have to defend a system that was built to be open and accessible (not secure), and there are almost limitless perimeter access points (and growing with the explosion of new technologies, such as mobile platforms and business models). As will be discussed in greater detail below, the Return on Investment (ROI) from cyber security investments is difficult to demonstrate, as it is exceptionally difficult to show what might have happened if a particular investment had not been made. Finally, the law enforcement community is badly outgunned by the attackers – estimates are that less than 2% (far less) of cyber attackers have been successfully prosecuted.[6]

So attacks are cheap easy and profitable. Defense almost inherently lags behind attack tools, ROI is difficult to demonstrate for things that are prevented, and successful law enforcement is virtually non-existent (despite Herculean efforts on the part of the law enforcement community). Considered in this comparative light, current incentives are not adequate.

D. The Adequacy of Incentives Depends on How One Defines the Risk, And the Term Adequacy – But a Rebalancing of Cyber Security Incentives Is Obviously in Order.

The empirical evidence clearly shows that there are tremendous incentives for private entities to invest in cyber security.

The Ponemon Institute has been tracking private sector cyber security investment for several years and their tracking study demonstrates that private sector investment in cyber security overall has doubled in the last 5 years from approximately $40 billion to $80 billion a year.[7]

To put this in perspective, the entire budget for the department of Homeland Security, including immigration, TSA, FEMA, everything, is just short of $60 billion a year.[8] The private sector is spending $80 billion on cyber alone.

On the other hand, PricewaterhouseCoopers's annual "Global Information Security Survey," which is broken down sector by sector regularly, has demonstrated that over the past several years nearly half of private sector entities have been forced to either defer or reduce their investment in cyber security, and the most prominent reason for

---

[6] Regoli, Robert M., and John D. Hewitt. "Exploring Criminal Justice: The Essentials." Jones and Bartlett Publishers: Sudbury, MA. 2010.

[7] Ponemon, Larry. Ponemon Institute IT Security Tracking Study Estimates. Feb. 2012.

[8] U.S. Department of Homeland Security. "Department of Homeland Security Budget in Brief: FY 2012." Oct 2011. Web. <http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf>.

these deferrals and reductions is economic.[9] This demonstrates that even within sectors, there are wide differences related to the economic incentives affecting cyber security investment.

The question of what constitutes "adequacy' is even more problematic. As will be discussed in greater detail below, government and industry, for fully appropriate reasons, have substantially different basis for judging what constitutes "adequate" security.

Moreover a lack of understanding of the state-of-the art of cyber security has often led some to use inappropriate metrics to assess what constitutes "adequate" security. For example, it is not unusual to hear the bemoaning of cyber breaches, with the apparent assumption that if a cyber system has been penetrated, or breached, that the security was *per se* inadequate and that the owner/operator of the system is *per se* negligent. This is a superficial and incorrect analysis that does not correspond to the modern cyber environment.

As explained above, the incentives favoring the attack community vastly outweigh the defense community, and the cyber systems were designed originally with little or no focus on security (a situation that largely continues to this day). All this has led to the common understanding among cyber professionals that there are really only two types of operators of cyber systems: there are those who know they have been successfully breached, and those who don't know they have been successfully breached.

As indicated above, breaching a system is not an appropriate metric, however, as to whether security is adequate or not. Adequate defenses may exist post the perimeter breach. A subsequent Notice of Inquiry might profitably analyze this complex issue more fully.

Notwithstanding the subtleties of fully answering the question posed, the bottom line is that with cyber incentives systemically out of line, losses mounting, and many companies having to defer or reduce cyber investment due to economic realities, the development of a new and powerful set of cyber security market incentives is in order.

2. Do particular business sectors or company types lack sufficient incentives to make cybersecurity investments more than others? If so, why?

A. Companies with Regulatory Mandates Do Not Fare Perceptibly Better with Respect to Cyber Security Than Less Regulated Firms.

Some sectors already have regulatory systems in place to mandate the adoption of

[9] PricewaterhouseCoopers. "The Global State of Information Security." Rep. 2008.

government approved cyber security standards and practices. There is a present ideology that holds that regulatory mandates are/should be a most effective incentive for cyber security. However, the facts do not bear out this assumption.

The federal government, if thought of as a sector, would be subject to the most direct and easily enforceable "sector wide" cyber security regulations in the economy. Yet, cyber attackers have successfully attacked almost every division of the federal government.

This is not a unique characteristic of government. Other sectors subject to highly regulatory cyber security requirements have fared no better than the comparatively non-regulated sectors.

For example, the health care industry is one of the most highly regulated sectors, including for cyber security. Yet, a series of studies have found that it is one of the least effective sectors on cyber security.

In 2009, the President's Stimulus package directed $38 billion dollars to the health care industry specifically for the purpose of creating electronic health records, and HHS followed up with the issuance of regulations for these systems, including for security.[10]

However, a 2013 study by the Washington Post found that the "health care industry is among the most vulnerable to cyber attack."[11]In their 2012 annual review of cyber security, Verizon found that "health care ranks near the bottom of the list of industries in terms of cyber security."[12] And a 2012 Johns Hopkins study concluded: "health care is the industry with the least regard, understanding or respect for cyber security…[and is] characterized by routine failure to fix aging technology and a culture where doctors, nurses and health care workers sidestep basic security measures, such as passwords, in favor of convenience."[13]

Neither the government, nor the health care sectors are populated by bad or

---

[10] See the American Recovery and Reinvestment Act of 2009, Division A, Title XIII, Subtitle D, also known as the HITECH Act (Pub.L. 111–5), and the Health Insurance Portability and Accountability Act ("HIPAA") (Pub.L. 104–191), and amendments as well as HIPAA/HITECH Regulations 42 CFR Parts 412, 413, 422 et al.

[11] O'Harrow, Robert. "Health-care sector vulnerable to hackers, researchers say." Washington Post. 25 Dec. 2012. Web. < http://wpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html>.

[12] Verizon. "2012 Data Breach Investigations Report." Rep. March 22, 2012, p.3. Web. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf>.

[13] O'Harrow, Robert. "Health-care sector vulnerable to hackers, researchers say." Washington Post. 25 Dec. 2012. Web. <http://wpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html>.

incompetent people. Indeed, these sectors tend to attract highly intelligent, skilled and motivated people. However, they stand as clear examples that a standards-based system lacking adequate attention to the overall incentive system in the culture will fail.

B. Cyber Security Is Different Than Consumer Product Safety.

There is a core misunderstanding that cyber security is akin to consumer product safety issues of the last century, that what is needed is "to get organizations up to standard." Advocates of this model tend to use analogies, such as federal mandates for seatbelts or air bags, pointing out that consumers' security was enhanced when the federal government mandated the installation of these security devices in cars. The major difference between seatbelts and cyber security is that no one was attacking the cars.

Our cyber systems are not yielding to attackers because they are bad systems. In fact, they are near miracle systems when viewed with any historic perspective. We have a cyber security problem because, as we definitively proved in the above answer, there are overwhelming incentives favoring the attack community over the defense community.

While coming up with a set of nationally determined standards may well be a useful exercise, assuming that this framework will be, by fiat, "adequate," let alone sufficient to address our nation's cyber security issues, is, at best, uncertain. The reality is that the problem is far more complex than a set of standards can address without extensive work addressing the misplaced economic incentives.

It is well known that cyber systems are being attacked all day and every day. Yet, despite this environment of constant cyber attack, there has never been a single instance of cyber attack even approaching the catastrophic level described in the Executive Order. Moreover the likelihood of such an attack being successful is "remote" due in large part to current defenses.

This success in protecting our critical infrastructure, while not perfect, is due in large part to the flexibility generated in the current system, which relies on voluntary partnerships within industry, and who can understand and manage these systems best. These partnerships can use their intimate knowledge plus information provided, at times by the government, to respond to rapidly emerging cyber threats in a fashion they believe can best protect the system.

This ability to be responsive to the situation on the ground, without having to worry about complying with a pre-set federal standard, is especially critical in the cyber security space, wherein infrastructure owners and operators need to be responsive to novel situations that evolve constantly. In such instances, it is critical that owners and operators dealing with a major attack are focused first and foremost on what needs to

be done to mitigate the attack, and not the reading of a pre-set performance requirement.

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

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

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

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

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

The bottom line is that the traditional regulatory system of enforcing standards maybe ill suited to address a complex and quickly evolving issue like cyber security,y even in those sectors that operate within a general regulatory model. However forbearance or modification of regulations for recognized "good actors" in regulatory sectors can be a powerful incentive to promote cyber security, and there is no necessity that the

regulatory modifications concern security, just so long as they are perceived as beneficial enough for the target entity to modify their security practices. See Appendix B for a list of existing programs that could be adapted or modified for cyber security purposes.

C. Sectors Where There Is a Strong Business Case for Cyber Security Seem to Do Better with Respect to Cyber Security.

The sectors who seem to do best at cyber security are those who address cyber security as a core business competency, meaning one for which they are economically compensated. The Defense Industrial Base (DIB) could be considered a case in point. The DIB companies compete for business in a large part based on security. As a result, they have strong economic incentives.

Major DIB companies are interested in securing their systems, not to just prevent governmental interference or loss (although these too are motivators), but, rather, they realize that by keeping ahead of the cyber threat, they will develop innovative products and solutions that will enhance their market position. Major financial institutions and some others with similar perspectives have similar successes.

The annual PricewaterhouseCoopers "Global State of Information Security Survey" regularly documents that regulations are not the biggest driver for cyber security even in highly regulated sectors.[14] Rather, these studies document a movement toward business orientations.[15]

3. How do businesses/your business assess the costs and benefits of enhancing their cybersecurity?

A. For the Private Sector, Security Benefits Are Measured Primarily in Economic Terms.

Most critical industry companies are publically traded organizations. In the United States, these companies operate under the legal obligation to maximize shareholder value.[16] As a result, companies assess the costs and benefits of all security investments

[14] PricewaterhouseCoopers "Global State of Information Security Survey: 2011" 28 Sept. 2010. Web. <http://www.pwc.com/gx/en/forensic-accounting-dispute-consulting-services/state-information-security-survey-2010.jhtml>.

[15] PricewaterhouseCoopers. "Lost in Translation? Exploring the roots of miscommunication: strategies to ensure Information Security is on your Board's Agenda." 20 Oct. 2010. Web. <http://www.ukmediacentre.pwc.com/imagelibrary/detail.aspx?MediaDetailsID=1816 >.

[16] Dodge v. Ford Motor Co., 170 N.W. 668 (Mich.1919); Carlton Investments v. TLC Beatrice International Holding, Inc., 1997 Del. Ch. LEXIS 86, 45 (ct. of Chancery, New Castle May 30, 1997).

on a risk-management basis, balancing the costs of security against the economic costs of security enhancements. Essentially, this is a straight up economic calculation.

For example, it is well known that retail entities routinely are aware that a certain percentage of their inventory is "walking out the back door" every month. While no company likes to lose this value, they tolerate a certain percentage of this insecurity as a cost of business. If 10% of the inventory is walking out the back door, this will be tolerated if it has been determined that it would cost 11% to hire the guards and install the cameras, etc., to reduce this cost of insecurity.

Businesses assess the costs and benefits of enhancing cyber security – as U.S. law requires them to do[17] – on the basis of what will maximize shareholder value.

B. Government Assesses Security Benefits on an Economic Plus Basis.

Government, on the other hand assesses the costs and benefits on a different basis. It is the government's Constitutional role not to maximize economic value, but to provide for the "common defense."[18] As a result, although government does have economic considerations when they assess security's costs and benefits, they also have important extra-economic issues, such as national security or individual privacy and civil liberty protection.

C. Although Government and Industry Share Cyber Networks, They Do Not Share an Identical System for Assessing Cyber Risk.

The cyber systems we are considering in this NOI are a shared network of networks. It's important to appreciate that although government and industry the basis upon which risk is analyzed share the cyber systems is aligned but not identical. Although both industry and government are interested in a risk-based system to manage cyber security, they assess risk on a basis that is different in important ways.

D. This Difference Is Especially Important in Considering Catastrophic Cyber Risk.

Clearly analyzing this difference in understanding risk becomes especially important when one considers the sorts of catastrophic cyber events described (twice) in the President's Executive Order and cited by Administration officials, such as former Secretary of Defense Leon Panetta.[19]

Private companies generally do not assess costs and benefits against the prospect of

---

[17] Ibid.

[18] "The Constitution of the United States," Preamble.

[19] Panetta, Leon. "Georgetown University Speech." Georgetown University. 6 Feb. 2013. <http://www.defense.gov/speeches/speech.aspx?speechid=1747>.

nation-state attacks. Expecting private companies to deploy – on a permanent basis – cyber defenses capable of withstanding attacks by nation states is unprecedented, unreasonable and unsustainable.

It should be clear that defending infrastructure against a nation-state attack, including one engaged by proxy, is not the responsibility of a private corporation. An attack sponsored by a nation state on infrastructure in another nation-state's jurisdiction, whether catastrophic or otherwise, is functionally an act of war, even if the legalities of this application have not been fully defined in the cyber space.

This issue was decided long ago with the emergence of the nuclear industry. Nuclear plants owned by private companies (although operating under strict government regulation) were expected to protect themselves against civilian attack, but the "design basis threat" from nation states was clearly identified as outside the role of the private company. The EO, nor any other document we are aware of offers any rationalization for why this historic precedent does not apply in cyber space.

Not only would expecting private companies to defend against nation state attacks be unprecedented, but also it would be unreasonable economically. In January 2012, Bloomberg and the Ponemon Institute released a study of 6 critical infrastructure sectors and reported on average that increasing private investment to prevent against catastrophic attacks would require a 900% increase in cyber security spending. This sort of investment to guard against what amount to acts of war (which the National Intelligence estimate suggests is a "remote risk") is clearly uneconomic and unsustainable.[20],[21]

4. What are the best ways to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face?

A. Private Sector Cyber Investments Are Made At the Corporate Level, Not the Sector or National Level, And, Hence A Single Sector or National Standard May Be Inadequate.

As illustrated above, the best way to encourage business to make investments in cyber security is to make these investments economically beneficial to that business. It is important to note that private sector cyber security investments are never made on

[20] Domenici, Helen, and Afzal Bari. "The Price of Cybersecurity: Improvements Drive Steep Cost Curve." Ponemon Institute-Bloomberg Government Study, 31 Jan. 2012.

[21] Clapper, James R. Statement to the House Permanent Select Committee on Intelligence. "Worldwide Threat Assessment of the U.S. Intelligence Community." Hearing. April 11, 2013. Web. <http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20WWTA%20US%20IC%20SFR%20%20HPSCI%2011%20Apr%202013.pdf>.

a national or even sector basis.

Private sector cyber security investments are made on a company-by-company basis (sometimes division-by-division or smaller).

As a result, defining a national baseline standard, while potentially beneficial, is not an adequate basis for determining national cyber security.

Even within industry sectors, different businesses have different systems, cultures, partnerships and business plans.

B. A Better System Would Be to Provide Incentives to A Range of Use Globally Determined Standards and Practices Allowing Private Companies to Choose which Effective Standards Best Meet Their Business Case.

Government ought to provide incentives for voluntary adoption of any of a variety of the globally developed standards and practices, so long as the standards and practices have been empirically proven to be effective.

In 2011, the ISA co-authored, along with the U.S. Chamber of Commerce, TechAmerica, Business Software Alliance, and Center for Democracy and Technology, a pan-trade association white paper, entitled, "Improving Our Nation's Cybersecurity through the Public-Private Partnership." Together, this broad-based industry coalition endorsed leveraging the current global standard setting process over the development of a "U.S." process:

> "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 the existing system of standards development rather than replace it with one that has a distinct bias in favor of national or participant 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.

"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…as opposed to creating new standards. Naturally, varying standards formulas will provide differing levels of security and likely at different cost levels."

Accordingly, it is recommended that "Government and industry [] utilize existing standards and work through consensus bodies to develop and strengthen international standards for cybersecurity." The U.S. government, via various entities (including NIST), already plays an active role in their development and should maintain that participation.[22]

Indeed, the creation of a single national standard, even segregated by sector is too limiting. Rather, the issue ought to be, is this standard, practice, or measure effective.

Providing incentives based on proven effective international standards, rather than adoption and adherence to a "U.S. Framework" or performance requirements, has additional advantages. A "U.S. Framework" and performance requirements would only heighten skepticism by global customers regarding the U.S. government's access to their corporate or consumer data, would surely impact American companies' global competitiveness and would most likely result in copycat policies in other countries.

[22] Internet Security Alliance, Business Software Alliance, TechAmerica, U.S. Chamber of Commerce, and Center for Democracy and Technology. "Improving Our Nation's Cybersecurity through the Public-Private Partnership." White Paper. March 2011. Web. <http://isalliance.org/publications/2C.%20Industry-Civil%20Liberties%20Community%20Cybersecurity%20White%20Paper%20-%20Improving%20our%20Nation's%20Cybersecurity%20through%20the%20Public-Private%20Partnership%20-%203-2011.pdf>.

Rather, the U.S. government ought to devote its resources to funding the analysis and evaluation of internationally developed, existing, consensus-based standards that are market-available and then provide incentives for organizations to implement the standards that are determined to be effective. Remember, cyber networks and infrastructure constitute a global system wherein 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. 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 should not and cannot deliberate public policy with merely a segmented, national lens.

C. A System of Incentives Tied to a Sliding Scale for Effectiveness.

Systems are neither entirely secure, nor insecure. Correspondingly, security controls for these systems often have different levels of effectiveness. Accordingly, security control effectiveness can and should be measured on a sliding scale. When it comes to medication, often the most effective drugs are the riskiest and require that they be administered during a hospital stay under a doctor's supervision. Less risky medications, that tend to be less effective, can be dispensed with a prescription. And even less risky drugs, with the least amount of effectiveness, can be purchased over-the-counter at a pharmacy by a consumer.

A similar sliding scale could also apply in cyber security. Such a sliding scale of effectiveness would be related to costs; often more effective methods are more costly. Accordingly, those that deploy the more effective/more costly controls would receive a higher level of incentive; such a model is entirely scalable. This scaling effect of cyber interventions is not problematic for an incentive model because incentives too can be scaled. For example, upon establishing a sliding scale where levels of A, B, and C are set to correspond with different levels of effectiveness, then those that achieve an "A" level could receive a 5% tax credit, those that achieve a "B" level could receive a 3% tax credit, and those that receive a "C" level could receive a 1% tax credit. Such a scale could be applied to other incentives, such as procurement preferences and litigation/liability benefits.

In sum, once the Government determines the effectiveness level of a particular method, then an appropriate menu of incentives could then be tied to the particular security level adopted, thus, encouraging additional cyber security investment.

5. How do businesses measure success and the cost-effectiveness of their current cybersecurity programs?

The ISA, in conjunction with its partners at the American National Standards Institute (ANSI), have made the issues addressed in this question a priority for many years. The answer to the question varies greatly from business to business, with some sophisticated enterprises demonstrating a broader and more effective conceptualization of how to measure cyber costs and effectiveness, while many others have an excessively narrow conceptualization of the issue.

For example, ISA membership consists of some of the most cyber sophisticated organizations in the world. ISA endorses, and many ISA members utilize, an enterprise-wide, risk-based approach to handling cyber security risk.

Enterprise-wide risk management means analyzing cyber issues from the unique perspectives of the functional heads across the enterprise, such as the human resource manager, the operations team, the legal and compliance offices, as well as the risk management and communications operations. Such an approach 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 and/or other senior executives. Together, these cross-functional teams identify and evaluate risks, which are then placed into context based on their potential impact, velocity, and/or probability. Senior Executives participate in this process, which has been communicated down from the Chief Executive Officer and Board of Directors.

On the other hand, A 2008 Deloitte study revealed 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.[23]

This same study also described how 65% of U.S. 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).[24]

The 2008 Carnegie Mellon University-CyLab study also provided alarming details about the state and structure of enterprise risk management of cyber security.[25] The study pointed out that:

- 83% of corporations do not have a cross-organizational privacy/security team.

[23] Deloitte. "Information Security & Enterprise Risk 2008." Presentation to CyLab Partners Conference, Carnegie Mellon University, Pittsburg, PA, October 15, 2009.

[24] Deloitte. "Information Security & Enterprise Risk 2008." Presentation to CyLab Partners Conference, Carnegie Mellon University, Pittsburg, PA, October 15, 2009.

[25] Westby, Jody. "Governance of Enterprise Security Study: CyLab 2008 Report." Carnegie Mellon CyLab. December 2008.

- 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.

To address these problems, the Internet Security Alliance entered into a collaboration with American National Standards Institute to develop a model for cyber security risk management. Beginning in 2006, the ISA-ANSI project involved more than 60 private entities and 13 government agencies. Every two years since, ISA-ANSI have released publications concerning cyber risk management. Currently, there are three publications, with a fourth scheduled to be published in the coming months.

The first two publications, "The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask"[26] and "The Financial Management of Cyber Risk: An Implementation Framework for CFOs,"[27] 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. This 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.

Following the success of these two publications, ISA and ANSI began collaboration on a third publication with the Santa Fe Group that focused exclusively on cyber risk management in the health care space. This publication, entitled, "The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security," builds upon the earlier enterprise-

[26] Internet Security Alliance and the American National Standards Institute. "The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask." 2008. Web. <http://isalliance.org/publications/1A.%20The%20Financial%20Impact%20of%20Cyber%20Risk-%2050%20Questions%20Every%20CFO%20Should%20Ask%20-%20ISA-ANSI%202008.pdf>.

[27] Internet Security Alliance and the American National Standards Institute. "The Financial Management of Cyber Risk: An Implementation Framework for CFOs." 2010. Web. <http://isalliance.org/publications/1B.%20The%20Financial%20Management%20of%20Cyber%20Risk%20-%20An%20Implementation%20Framework%20for%20CFOs%20-%20ISA-ANSI%202010.pdf>.

wide framework and was released in 2012.[28] A fourth publication that examines the cyber security risk management strategies of leading organizations in the aerospace and defense, advanced technology, and financial services industries will be published later this year.

Since the release of these publications, there has been a noticeable shift in the private sector toward adoption of the enterprise-wide, cyber risk management approach that ISA and ANSI have advocated. The CMU CyLab studies that are produced every two years have tracked this shift. As noted, in 2008, only 17% of surveyed corporations had established cross-organizational teams to "manage privacy and security risks," but by 2012, that number had jumped to 72%. The recent "Governance of Enterprise Security: CyLab 2012 Report" also detailed that during this four year span, there had been a "noticeable increase" in the number of corporate boards with Risk Committees responsible for privacy and security risks, rising from a mere 8% in 2008 to 48% in 2012.[29]

Despite this progress, substantially more needs to be done to elevate the understanding of the nature of the cyber threat as more than just a technical issue, but an enterprise-wide, risk management issue. For example, the PwC "Global State of Information Security Survey: 2013" found that senior management was often seen as a major obstacle in managing the cyber threat, often an obstacle equivalent to that of economic constraints.[30]

As is described in greater detail in question 7, senior managers are often faced with strong economic imperatives to deploy increasingly insecure technologies and business operations. Most of these deployments are motivated by short-term economic gain, while possibly not fully accounting for the longer term security risks.

Clearly substantial additional work needs to be done to educate senior managers and Boards as to the true nature of the cyber threat and how to appropriately measure its long-term impacts on their company.

---

[28] Internet Security Alliance, et al. "The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security." 2012. Web. <http://isalliance.org/publications/1C.%20The%20Financial%20Impact%20of%20Breached%20Protected%20Health%20Information%20-%20A%20Business%20Case%20for%20Enhanced%20PHI%20Security%20-%202012.pdf>.

[29] Westby, Jody. "Governance of Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives are Managing Cyber Risks." Carnegie Mellon University CyLab. 16 May 2012. Web. <http://www.cylab.cmu.edu/outreach/governance.html>.

[30] PricewaterhouseCoopers. "The Global State of Information Security Survey: 2013" Sept. 2012. Web. <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml>.

6. Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make security investments or other investments that can be applied to security?

We have not had an opportunity to fully assess how other nations are using cyber security incentives. We are aware, however, of numerous examples of incentives that have been deployed by the U.S. Government to achieve pro-social goals. These examples along with how these incentives structure can be adapted are contained in a separately submitted "Appendix B: Adaptation of Other Incentives Models to Cybersecurity" and "Appendix C: General Principles Regarding the Use of Incentives in the President's Executive Order."

7. Are there disincentives or barriers that inhibit cybersecurity investments by firms? Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively? If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?

First with respect to business in general the answer is yes, there are massive incentives to be insecure in technology and business practice. The use of VoIP, as opposed to traditional telephony, as well as the use of long international supply chains, the move to cloud computing, off-shoring labor, and BYOD are just a handful of examples of technologies and business practices that offer compelling - sometimes competitively irresistible - economic incentives to adopt less secure technologies and business models.

For example the adoption of unified communications (UC) platforms, such as voice-over-Internet protocol (VoIP) mobile phones and tablets is one such example: "[W]hile unified communications offer a compelling business case, the strength of the UC solutions in leveraging the internet is also vulnerability. Not only are UC solutions exposed to security vulnerabilities and risk that the Internet presents, but the availability and relative youth of UC solutions encouraged malicious actors to develop and launch new types of attacks."[31]

A similar example of this phenomenon involves cloud computing. Just like VoIP and other unified communications platforms, cloud computing has emerged as one of the hottest developments in information technology, driven largely by perceived economic

[31] Internet Security Alliance. "Navigating Compliance and Security for Unified Communication" Rep. Internet Security Alliance, 2009, 21. Web. <http://isalliance.org/publications/6.%20Navigating%20Compliance%20and%20Security%20for%20Unified%20Communications%20-%20ISA%202009.pdf >.

benefits ranging from cost savings and efficiencies.[32] And like VoIP and UC, deployment security has fallen aside because of competitive pressures driving cost reductions. In fact, a recent survey found that while forty-nine percent of executive respondents had deployed a cloud solution, sixty-two percent of them acknowledged having little or no faith in the security of the data in the cloud.[33]

In terms of barriers, one barrier to cybersecurity investment is the lack of timely, actionable intelligence provided to industry on existing and emerging threats. One example of where timely intelligence incentivized industry action is the development of Secure BIOS solutions. Lack of awareness of this emerging threat to BIOS integrity had led to few solutions and relatively little market pull for the creation of Secure BIOS solutions to protect IT platforms. Once government had provided briefings to industry to establish severity of the threat, industry leaders were able to quickly mobilize resources to create and deploy solutions to meet this threat. Indeed, a well-informed private industry community will more readily apply resources to develop and implement cybersecurity solutions.

8. Are incentives different for small businesses? If so, how?

Small businesses working within the critical infrastructure and key resources (CIKR) sectors are disadvantaged by incentive misalignment. As potential targets of cyber attacks, we should recognize that small businesses (in contrast to large businesses) tend to have more pronounced concentrations of intellectual property, thus, facilitating exploitation of that information. In addition, we should recognize that many leading technical advances are generated within small businesses. Collectively, these considerations suggest that the "ripeness" of small business as a cyber attack target is especially pronounced. Combined with potentially immature cyber practices, and insufficient cyber security investments – cyber attacks against small business CIKR participants may yield significant rewards. In order to effectively incentivize small business participation in the NIST framework, special consideration should be given to tiered levels of incentives that would be sufficient to provide meaningful assistance to small businesses to adhere to the NIST framework standards (see ISA Response to Question 4 for a more detailed discussion of tiered incentivization).

9. For American businesses that are already subject to cybersecurity requirements, what is the cost of compliance and is it burdensome relative to other costs of doing business?

[32] Yoo, Christopher. "Cloud Computing: Architectural and Policy Implications" Rep. Technology Policy Institute, January 2011, 6.

[33] PricewaterhouseCoopers. "PwC 2011 Global State of Information Security Survey." Rep. PricewaterhouseCoopers, 2010. Web. <http://www.pwc.com/giss2011.2010>.

For the past several years, the Ponemon Institute has been tracking private sector spending related to cyber security, including spending on computer security technologies, such as firewalls, intrusion detection systems, etc.; governance and control activities, such as traffic monitoring, compliance, and training; security management outsourcing; and securing industrial control systems. According to a recent Ponemon study, private sector spending by U.S. companies on cyber security has in fact doubled in the last 5 years to approximately $80 billion dollars for 2011.[34] By comparison, the official spending request for the entire Department of Homeland Security during that same time frame, for calendar year 2012, was only $57 billion.[35] This was the complete requested budget, inclusive of FEMA, TSA, ICE, etc.

One example of where the cybersecurity-related regulatory cost is overly burdensome is related to the DHS implementation of the Chemical Facility Anti-Terrorism Standard (CFATS). Specifically, the cybersecurity components of the CFATS audit regime and process are overly repetitive across an impacted business and the oversight process is manpower intensive. More effectively partnering with industry in the development of any regulatory regime would enable a more efficient and effective audit process for both industry and government stakeholders.

10. What are the merits of providing legal safe-harbors to individuals and commercial entities that participate in the DHS Program? By contrast, what would be the merits or implications of incentives that hold entities accountable for failure to exercise reasonable care that results in a loss due to inadequate security measures?

Liability is one of the most hotly discussed incentives in the cyber security world, and we believe liability protections can have a positive effect on some cyber security decisions. For example, shielding entities from liability stemming from disclosures made in good faith as part of an information sharing program may ameliorate some concerns with respect to sharing valuable information. However, even in this case, it does not provide an affirmative incentive, since an entity sharing this data gains nothing tangible and would be no better off from a risk perspective than if they had not shared the information in the first place.

For liability protection to have a strong positive impact, it must be perceived as providing a useful benefit. For example, some previous legislative proposals have suggested protections from punitive damages in cases where actual damages would "wipe a firm out," and so the supposed liability benefit is functionally nil. Moreover,

[34] Ponemon, Larry. Ponemon Institute IT Security Tracking Study Estimates. Feb. 2012.

[35] U.S. Department of Homeland Security. Department of Homeland Security Budget in Brief: FY 2012. Oct. 2011. Web. 6 Feb. 2012. <http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf>.

liability protections are subject to extensive court challenges, and the court costs arising from defending a case may well eliminate the supposed advantage of the liability protection.

While liability protections may be useful in some cases, it is more likely that direct economic advantages (e.g., regulatory forbearance, tax benefits, streamlined permitting, preferential access, etc.) would have a more positive motivating effect.

As to the issue of holding companies responsible for not providing reasonable care as suggested above, a single reasonableness standard is difficult to determine given the ever-evolving threat and the lack of clarity as to what "adequacy" means. It may well be that this is an issue that varies so considerably given the uniqueness of targets and attacks, that such a single standard may be elusive.

For example it is doubtful that standards and practices alone will be adequate to prevent today's more sophisticated attacks, such as the so-called APT, and research shows that these more sophisticated attacks are becoming the norm and not the exception.

11. What would be the impact of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance in relevant sectors? How can liability structures and insurance, respectively, be used as incentives? What other market tools are available to encourage cyber security best practices?

These questions are addressed in ISA Response to Question 6 as well through review of ISA Appendices B and C.

12. Should efforts be taken to better promote and/or support the adoption of the Framework or specific standards, practices, and guidelines beyond the DHS Program? If so, what efforts would be effective?

It is impossible to answer what should be done beyond the DHS program without first having a solid idea of what will be in the DHS program.

That being said, ISA has offered an alternative to the DHS, U.S. centric, model based on the current global standards regimes as measured for effectiveness (see IS Response to Question 4B).

Additionally, ISA has long proposed a unique model for providing a series of incentives for information sharing (see "Appendix D: 'A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels,' by ISA Board Member Jeffrey Brown (Raytheon)"), some of which are quite compatible and comparable with

those offered by the Enhanced Cybersecurity Services Program described in Section 4(c) of the EO.

Finally, an educational program targeted to senior executives and Board of Directors that is modeled on the ANSI-ISA program for financial management of cyber risk (see ISA Response to Question 5), which addresses cyber security on an economic basis, will, we believe, be far more cost-effective than expensive public service announcements (PSAs) and other general population advertising and outreach.

13. In what way should these standards, practices, and guidelines be promoted to small businesses and multinationals, respectively, and through what mechanisms? How can they be promoted and adapted for multinational companies in various jurisdictions?

The best way to promote the adoption of standards and practices is to make the use of these standards and practices economically valuable for the user. As indicated above, the evaluation of value will be made independently by each organization, not on a sector-wide basis. The answers provided above, and in the attached appendices provide multiple potential pathways to be considered as well as a scale of principles by which the effectiveness of the incentives ought to be evaluated. If there is an economic benefit, organizations will voluntarily continue to raise the bar in their own self interest.

As to the international question, we refer you back to our proposal in ISA Response to Question 4, which suggests that a better use of time and effort would be to take the standards and practices that are already (and continually) being globally developed and fund independent evaluations of these standards and practices for their relative effectiveness. Incentives can then be offered on an increasing scale to companies that voluntarily elect to adopt the more secure practices/scale levels. We, and many others, have serious concerns regarding a U.S. centric system.

The Internet Security Alliance

Appendix A: Internet Security Alliance (ISA) Board of Directors List

March 28, 2013 Notice of Inquiry
of the
U.S. Department of Commerce, National Telecommunications & Information Administration

April 29, 2013

Contact:
Larry Clinton, Internet Security Alliance (ISA) President & CEO
Phone: (703) 907-7090
Email: lclinton@isalliance.org
Web: www.isalliance.org

About the Internet Security Alliance (ISA):
ISA is a multi-sector trade association with membership from virtually every one of the designated critical industry sectors, including substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries. ISA focuses exclusively on cybersecurity and cybersecurity related issues as is embodied in its mission, which is to create a sustainable system of cybersecurity by combining advanced technology with economics and public policy.

Founded in 2000 in collaboration with Carnegie Mellon, ISA is also unique in that combines the thought leadership that might be found in a "think tank," with advocacy one would expect from a trade association, and operational security programs that might be found in a professional association.

* * * * *

Appendix A: Internet Security Alliance (ISA) Board of Directors List

(April 2013)

Chairman
Tim McKnight, Executive Vice President/Enterprise Information Security and Risk, **Fidelity Investments**

First Vice Chairman
Jeff Brown, Vice President of Infrastructure Services and Chief Information Security Officer for Information Technology, **Raytheon**

Second Vice Chairman
Gary McAlum, Senior Vice President and Chief Security Officer, **USAA**

Marcus Sachs, Vice President of National Security Policy, **Verizon**

Thomas Quinn, Managing Director, Chief Information Security Officer, **BNY Mellon**

(Lt. Gen. Ret.) Charlie Croom, Vice President of Cyber Security Solutions, **Lockheed Martin Corporation**

Russell Koste, Director of Identity, Intelligence and Network Defense**, Northrop Grumman.**

Rich Baich, Chief Information Security Officer**, Wells Fargo**

Larry Trittschuh, Director, Global Information Security Operations**, General Electric**

Tim McNulty, Cylab Associate Vice President of Government Relations, **Carnegie Mellon University**

Jeff Schilling, Director for the Incident Response Practice**, Dell SecureWorks**

Gene Fredriksen, Senior Director and CISO, **Tyco International**

Thomas Kelly, Director of Information Security - Assessments and Vulnerabilities, **Boeing**

Julie Taylor, Vice President, Deputy Operations Manager, **SAIC**

Joe Buonomo, President and Chief Executive Officer, **Direct Computer Resources**

Siobhan MacDermott, Chief Policy Officer, **AVG**

Brian Raymond, Director of Tax, Technology and Domestic Economic Policy, **National Association of Manufacturers**

Richard Knowlton, Group Corporate Security Director, **Vodafone Group**

Larry Clinton, President & CEO, **Internet Security Alliance**

Incentive Targets and Regulatory Authority	Incentive Types	Description	How This Can Be Adapted for Cybersecurity
Provision of Internet Services Authority: Digital Millennium Copyright Act of 1998	• Liability Protection – "Safe Harbor"	In order to clarify an Internet Service Provider's legal exposure and to encourage provision of Internet services, the Digital Millennium Copyright Act provides liability protections to ISPs, namely safe harbors from liability for their users' actions with respect to copyright infringement provided that ISPs adhere to certain requirements.	Similar to CISPA and other Congressional bills, clarify the liability and provide safe harbors for ISPs to intervene and sandbox malicious communications traversing its wire to another ISP end-user
Provision of Wireless Broadband Services to Rural U.S. and other non-profitable areas Authority: Obama Administration's June 2010 memo "Unleashing the Wireless Broadband Revolution" and the Feb 2011 Presidential "National Wireless Initiative"	• Freeing up of Govt Spectrum • Voluntary Incentive Auctions • $5B allocation for product purchase (rural direct subsidy) • $3B R&D	To motivate Comms providers to supply wireless broadband to areas where it is not business justifiable (e.g., rural areas), the Administration urged both the U.S. Congress the DoC's National Telecommunications and Information Administration to "adopt proposals to improve the process for reassigning spectrum encumbered by Federal users to private use, grant authority for the FCC to hold incentive auctions, create governance structures and channel auction proceeds to manage the deployment and operation of a nationwide interoperable public safety broadband network, and spur innovation in wireless services by both providing for unlicensed access to wireless spectrum and funding critical research and development."	Tie Auctions to Cyber - Since there is no specific directive or law, but rather a nudging by the President for the U.S. Congress and the DoC's National Telecommunications and Information Administration to "adopt proposals to improve the process for reassigning spectrum…," part of the President's directive, at least with respect to the Department of Commerce, could be that those that integrate certain Framework measures, could then receive either exclusive invitation to the auction and/or reduced auction pricing to the extent legally feasible. Cyber Patriot Bonds - Since cybersecurity has been called the greatest national threat facing the United States, now replacing terrorism, much like in the past, the government could issue a series of Cyber Patriot Bonds that could be tied to Framework adoption costs and/or loans that are needed in order to implement the Frameworks

Incentive Targets and Regulatory Authority	Incentive Types	Description	How This Can Be Adapted for Cybersecurity
The Hiring of Longer-Term Unemployed Authority: Hiring Incentives to Restore Employment (HIRE) Act	• Tax Incentives	In order to motivate the business community to hire those that are longer term unemployed – those that have been unemployed for at least 60 days – the President and Congress enacted a law that cut the employer taxes for those businesses that hired such individuals. More specifically, employers that hired such individuals in 2010 qualified for a 6.2-percent payroll tax incentive, in effect exempting them from their share of Social Security taxes on wages paid to these workers after March 18, 2010 as well as $1000 business tax credit for year 2011 if the workers were retained for at least a year.	Similar to this effort, the President might consider asking Congress to pass a tax law in which corporations who have employees dedicated to implementing the Framework would receive a similar type of tax benefit. Such a bill could also provide for tax credits to certain eligible individuals that have a computer science background to receive training in cybersecurity.
Advantaging to offset disability, past discrimination, and/or to encourage small business growth Authority: The Veterans Benefit Act of 2003; Small Business: 15 USC 633 et seq; Women and Minorities: 15 USC 637; the Office of Federal Procurement Policy Act of 1974 (Pub. L. 93-400).	• Federal Procurement Advantaging	In order to provide assistance to small businesses, those that have been service disabled, and those that have been historically discriminated against (i.e., women and minorities), the federal government has set up federal procurement programs to aid these groups in obtaining federal procurement contracts.	Security Reliant Products - Where cybersecurity or IT is a key requirement in terms of purchasing, than those that have already adopted the framework prior to the bid should be provided exclusive bidding rights so that there is a reduced number of bidders and so that the bids submitted reflect the actual costs of building in security, and not just a lowest possible bid number. If a suitable bidder can not be found due to specifications other than cost, then the bids can be opened up to the general market. General Products - Much like the advantages provided to small business owners and businesses owned by disabled veterans, women, and minorities, businesses that adopt the Framework should receive comparable preference.

Incentive Targets and Regulatory Authority	Incentive Types	Description	How This Can Be Adapted for Cybersecurity
Airline Industry adoption of the "NextGen" Technologies (GPS and other air traffic control technologies) Authority: FAA Modernization and Reform Act of 2012 and Federal Credit Reform Act of 1990	• Preferential take-off and landing treatment • Low interest loans	The acts grant authority for the Secretary of Transportation to establish an equipage incentive program to equip US registered aircraft with NextGen technologies and capabilities. While the FAA act mentions the establishment of a "loan guarantee program," other incentives that are being considered include preferential take-off and landings for those equipped with NextGen technologies.	Preferential Treatment - Those that adopt the Framework could have expedited clearances (moved to the head of the line), expedited SCIF sponsorship (non-monetary sponsorship, just sponsorship that will allow for purchase and certification in a timely manner); cyber exchange programs through deputization to the NSA, FBI, DOJ Loans - For critical infrastructure segments such as banking, etc., that incur transactional costs equal to a certain percentage rate, they could receive discounted rates (e.g., for the banking industry: reduced overnight funds rate, reduced Federal Wire fee, etc.)

Incentive Targets and Regulatory Authority	Incentive Types	Description	How This Can Be Adapted for Cybersecurity
Incentivize Health Care Providers to Switch to Electronic Health Records (EHRs) Authority: HIPAA/HITECH and HIPAA/HITECH Regulations 42 CFR Parts 412, 413, 422 et al	• Monetary Payments/Incentives	In order to encourage health care providers to move to electronic based health records so that the records will be more readily available to patients and decrease paper related costs for federal and state agencies, the government has been providing direct monetary incentives to eligible healthcare professionals that do so in within a specific timeframe and that meet certain "meaningful use" requirements. For eligible professionals providing healthcare to medicare patients, payouts can reach as high as $44,000 per provider, released over a 5 yr period. For Medicaid, the incentive maximum per provider is $63,750. Effectiveness: Since the program started, the AMA has reported that over 125,000 healthcare providers have opted into the incentive based program.	Such a system of payout can be provided to those that adopt different security tiers tied to the Framework

Incentive Targets and Regulatory Authority	Incentive Types	Description	How This Can Be Adapted for Cybersecurity
Encourage Pharmaceutical Companies to Develop Treatment for Rare (Non-Profitable) Diseases Authority: Orphan Drug Act of 1983 and Amendments	• 7 yr Market Exclusivity Rights • Fast-Track Drug Approvals (streamlined permitting) • Access to Investigational New Drug Program • Waiver of FDA Fees • Tax Incentives • Grants	Under the Orphan Drug Act (ODA) "drugs, vaccines, and diagnostic agents" would qualify for orphan status if they were intended to treat a disease affecting less than 200,000 American citizens. In order to encourage the development of drugs for orphan diseases, the ODA included a number of incentives including seven-year market exclusivity for companies that developed orphan drug, tax credits equal to half of the development costs (later changed to a fifteen-year carry-forward provision and a three-year carry-back that can be applied in profitable year), grants for drug development, fast-track approvals of drugs indicated for rare diseases, and expanded access to the Investigational New Drug Program. The law was also later amended to waive FDA user fees. Effectiveness: In the USA, from January 1983 to June 2004, a total of 1,129 different orphan drug designations have been granted by the Office of Orphan Products Development (OOPD) and 249 orphan drugs have received marketing authorization. In contrast, the decade prior to 1983 saw fewer than ten such products come to market. In 2010, Pfizer established a division to focus specifically on the development of orphan drugs as other large pharmaceutical companies focused greater efforts on the orphan drug research.	Market Exclusivity/Fast-Track Approval - While patents provide certain levels of market exclusivity, products that are submitted as cyber critical by entities that have adopted the framework could be rushed to the head of the patent review process so that they can then be first to market as well as patent protected. Access to R&D - For companies that have adopted the Framework and also have appropriate security clearances, etc., they would have access to Federal Govt cyber R&D efforts with the ability to purchase these R&D streams at reduced costs (i.e., IP transfer)

Incentive Targets and Regulatory Authority	Incentive Types	Description	How This Can Be Adapted for Cybersecurity
Public-Private Partnership to Identify and Fix Dangerous Rail and Road Intersections/Crossings Authority: Highway Safety Acts and Surface Transportation Assistance Acts (aka the 23 U.S.C. 130 Program)	• Full Fed/State Payment for Dangerous Crossings Selected for Remediation • Liability Protection – Litigation Discovery Exclusion of Private Sector Identified Crossings Bisecting Private Sector Property	In order to reduce the amount of fatalities at railroad and road intersections/crossings, the Federal government enacted a program whereby it would fund the States to fix selected dangerous crossings that were self-identified by private sector owners and operators as dangerous. In order to assure private sector cooperation in identifying those crossings, the Federal government provided that the identifying documentation, etc., produced by the private sector would not be discoverable in either State or Federal litigation proceedings. Effectiveness: From 1973 to 2005, approximately $4B has been spent on 23 U.S.C. 130 program grade crossings. Program has been credited with dropping fatality rates at grade crossings by 70%. (Texas Transportation Institute Report)	In essence, through the non-disclosure provision of the RR program, it acts as a means to perform a self-audit without the risk of then having this audit be used against the entity that commissioned this audit. A self-audit privilege could be extended for those organizations that would like to spend the time and money to do an in-depth and comprehensive risk assessment to look for such things such as the APT. Such assessments are costly and coupled with the fact that such assessments can conceivably be used in State and/or Federal courts that a company was on "notice" of certain vulnerabilities, provides a disincentive to conducting one. A federal law that would bar such self-audits from being discoverable as in the case with the RR crossings both in Federal and State courts would incentivize such self-audits and corresponding remediation efforts. It would also have the benefit of allowing insurers to better quantify risk and set more purchasable premium rates for cyber insurance. Besides the Railroad industry, similar privileges have been extended to facilitate lawyer-client, doctor-patient communications, and in doctor to doctor morbidity and mortality reviews.

Incentive Targets and Regulatory Authority	Incentive Types	Description	How This Can Be Adapted for Cybersecurity
Enabling the Provision of Private Sector Generated Nuclear Power Authority: Price-Anderson Nuclear Industries Indemnity Act	• Utilization of Insurance • Partial Indemnity • Litigation incentives, such as case consolidation, automatic transfer to federal court… • Punitive Damage Exemption	When it became apparent that the private sector was refraining from entering the nuclear power generating business because companies could not obtain insurance to cover possible incident expenses at acceptable levels, the Federal Govt enacted the Price-Anderson Act wherein the Govt provided that if nuclear power companies purchased the highest level of insurance available, it would cover litigation costs beyond that using a revolving fund of user/generator fees. The Act also provided that companies were exempt from punitive damages and would receive litigation incentives, such as the required consolidation of cases and transfer to a single federal court. Effectiveness: Following its enactment, private sector companies entered into nuclear power generation.	The provisions of the Price-Anderson act both in terms of insurance purchasing as well as litigation incentives such as partial indemnity, case consolidation, case transfer to a single federal court, punitive damage exemption could be married with the incentives and provisions of the SAFETY Act, such as the incentives for designation v. certification, and could be adapted to the cybersecurity realm so that entities employing certain security measures tied to the Framework or that invent certain certified cybersecurity technologies would receive such benefits.

Incentive Targets and Regulatory Authority	Incentive Types	Description	How This Can Be Adapted for Cybersecurity
Environmental Protection	• Limited Liability for Owners of "Brownfields" that work to remediate hazardous sites • Choice of Hazardous Site Remediation Levels • Streamlined Permitting • Marketable Permits • Subsidies, Grants, Tax Exemptions	In order to encourage businesses to remediate and develop hazardous waste sites, to reduce carbon emissions, acid rain, etc., the U.S. Congress and EPA have developed a series of different programs wherein good actors would receive certain incentives described at left. Effectiveness: According to the EPA report cited below, "it is clear that economic incentives do provide the opportunity to achieve any given level of pollution control with substantial cost savings…At least 40 studies based on computer modeling of different scenarios for controlling pollution show what economic incentives should be more cost-effective than traditional regulations. One study (ICF, 1989) estimated that allowance trading in EPA's acid rain program could result in savings to effected utilities of $700 to $800 million per year over the long term. The actual cost savings now are believed to be at least twice this amount." (EPA Report, pp.ix-x). For Greater Detail: See the EPA's January 2001 Report, entitled "The United States Experience with Economic Incentives for Protecting the Environment"	Choice of Security Level Adoption - Similar to "Brownfields," corporations would be able to choose which security tier or level it would want to adopt and then would be eligible for a menu of market incentives tied to that particular tier. This would mean that the Framework would also have to be tiered. So that critical infrastructure and key resources (CIKR) providers can better understand and select from among these tiers and corresponding incentives, the Government should stand up a Cybersecurity Incentives Exchange using the Affordable Care Act's Healthcare Exchange as a model. The idea being that this exchange will list the incentives that are available for selection in a given sector, and, even further, within a particular tier of security. Such an Incentives Exchange could also play host company's self certifications / assertions that they are compliant with applicable provisions of the framework. In fact, such assertions would likely be part of the basis for determining incentive eligibility, in addition to CIKR standing, and associated sub-tiers. Marketing - Much like the marketable environmental permits (e.g., Energy Star, etc.), these certifications and designations could likewise be marketable with marketing efforts supported by the Government, Ad Council, etc.

The Internet Security Alliance

Appendix C: General Principles Regarding the Use of Incentives in the President's Executive Order

March 28, 2013 Notice of Inquiry of the U.S. Department of Commerce, National Telecommunications & Information Administration

April 29, 2013

Contact:
Larry Clinton, Internet Security Alliance (ISA) President & CEO
Phone: (703) 907-7090
Email: lclinton@isalliance.org
Web: www.isalliance.org

About the Internet Security Alliance (ISA):
ISA is a multi-sector trade association with membership from virtually every one of the designated critical industry sectors, including substantial participation from the aviation, banking, communications, defense, education, financial services, health care, insurance, manufacturing, security and technology industries. ISA focuses exclusively on cybersecurity and cybersecurity related issues as is embodied in its mission, which is to create a sustainable system of cybersecurity by combining advanced technology with economics and public policy.

Founded in 2000 in collaboration with Carnegie Mellon, ISA is also unique in that combines the thought leadership that might be found in a "think tank," with advocacy one would expect from a trade association, and operational security programs that might be found in a professional association.

ISA Board of Directors:
For a current list of the ISA Board of Directors, please refer to Appendix X: ISA Board of Directors, which has been submitted along with the ISA's Response and Appendices to the U.S. Department of Commerce, National Telecommunications & Information Administration's Notice of Inquiry.

Appendix C: General Principles Regarding the Use of Incentives in the President's Executive Order

1. ***Bridging the "Risk Gap" Between Industry and Government with Incentives***
    - The Presidential Executive Order (EO) asserts that it will be risk-based. Government and Industry have aligned, but not identical interests when it comes to risk. Government assesses risk in terms of its mandate to provide for the common defense. Industry assesses risk against its legal mandate to maximize shareholder value. As such, industry makes its investments for security on a primarily economic/commercial basis. Government has non-economic interests, such as national security, that it must consider in assessing the need for cyber security investment. This means Industry may have a higher tolerance of risk than that of the Government. In order to fill this risk tolerance gap, and secure the shared network of the Internet, incentives should be used.
2. ***It's the U.S. Government's Job to Protect Against Nation-State Attacks***
    - The EO cites catastrophic events that can result from cyber attacks. While these are technologically feasible, the chances of them occurring are, according to the National Intelligence Estimate, "remote," as only nation-states have this capability and capable nation-states lack incentive to carry out such attacks. Precedent, such as the design basis threat analysis in the nuclear industry, makes clear that defending against such attacks on critical infrastructure is a government, not private sector, responsibility. Moreover, a 2012 Bloomberg report has indicated that it would require a 900% increase in spending beyond the current spending of $80B (the entire DHS budget was only $59B for 2012) to defend critical infrastructure against this threat.[1],[2],[3] Clearly, it is unrealistic to assume the private sector can incur anything close to this degree of increased investment, and, thus, market incentives of a significant nature would be prudent to address this threat.
3. ***Being Breached Does Not Mean You Have Been Negligent***
    - It is widely acknowledged that adherence to standards and practices will not prevent sophisticated cyber attacks. There are now two types of companies: those that know that they have been successfully breached, and those that don't know they have been successfully attacked. Moreover, even if you have been breached, this does not mean that an attack has been successful; there are defenses, such as blocking outbound traffic, that can be used to negate attacks even once the perimeter has been breached. The notion that a breach has occurred and therefore the host has been negligent and deserves some sort of public sanction is unfounded. Moreover, such an approach can lead to anti-security behavior such as reducing private incentives to look for stealth attacks, as the reward for such discovery could be punitive action against them. Effective incentives should generate a collaborative atmosphere and do more than just promote perimeter defense, but motivate entities to be responsive to ever-changing attack methods.
4. ***Traditional Regulation Is A Bad Fit for Cyber Security***

[1] Domenici, Helen, and Afzal Bari. "The Price of Cybersecurity: Improvements Drive Steep Cost Curve." Ponemon Institute-Bloomberg Government Study, 31 Jan. 2012.

[2] Ponemon, Larry. Ponemon Institute IT Security Tracking Study Estimates. Feb. 2012

[3] U.S. Department of Homeland Security. "Department of Homeland Security Budget in Brief: FY 2012." Oct 2011. Web. <http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf>.

- For reasons having to do with the unique characteristics of the Internet, traditional regulation is ill-suited to creating a sustainable secure cyber system. History shows regulated sectors do not do better than less regulated ones with respect to cyber security. For example, the federal government has been subject to FISMA standards and regulations for a decade and yet has suffered numerous successful cyber attacks. Similarly, the health care system, though highly regulated, including for cyber security, has been shown by a range of studies (e.g., Washington Post, PwC) to be one of the worst in terms of cyber security.[4],[5] Traditional regulation is static, and technology and attack methods change constantly. Regulations take too long to become promulgated. Regulations tend to provide a ceiling, and not a floor, and are nation-specific, so that even if we developed a solid regulatory system, in a global world economy, it would be of little practical use. Incentives, on the other hand, can promote continued and progressive steps to address evolving cyber threats and on an enterprise- wide basis not encumbered by artificial nation state boundaries. Market incentives should be designed to motivate corporate entities to continually enhance their cyber security efforts because it makes good business sense, not just because it will achieve compliance with a government regime.

5. ***Incentives Ought to Be Available to the Current Globally Produced Standards and Practices Based on Independent Evaluation of Their Effectiveness***
   - The economy is now global, as are product sales and services. Therefore, any framework of measures should not only look to harmonize across Federal, State, and local governments, but also internationally. A patchwork of measures needlessly elevates costs of production and compliance, thus harming U.S. competitiveness. The Internet Security Alliance, the U.S. Chamber of Commerce, Tech America, Business Software Alliance and the Center for Democracy and Technology proposed an alternative model in the pan-industry White Paper on Cyber Security issued in 2011. This paper suggests that the current global system of standards, not a new U.S. standards regime, be utilized. This method will produce a multiple of standards and practices that may better fit the varying business plans of owners and operators. The varying standards ought to then be evaluated for their relative effectiveness, and governments should grant incentives to entities that voluntarily choose to adopt higher levels of effective standards. The key point being that who created the standard/practice are of little importance. The key question is how effective is the standard/practice. Given the global nature of commerce, the current system should be utilized and ongoing evaluations of the regimes should be funded by government with private industry left alone to select what system best fits their needs, considering the incentives that are associated with adopting higher level regimes.

     In instances, such as sectors already under government regimes for cyber security, these current systems should be "grandfathered-in" and only amended based on evaluations that amendments meet cost-effectiveness as well as other criteria specified in the EO. Duplicative or redundant regulations ought to be avoided.

---

[4] O'Harrow, Robert. "Health-care sector vulnerable to hackers, researchers say." Washington Post. 25 Dec. 2012. Web. <http://wpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html>.

[5] PricewaterhouseCoopers. "The Global State of Information Security." Rep. 2013.

6. ***For the Incentives to Be Truly Risk-Based, We Need to Be Clear About What Exactly We Are Trying to Incentivize***
    - The definition offered at the workshop suggested that the goal of the incentives was to encourage corporate entities to adopt the voluntary framework. However, since the framework has not been specified, even in preliminary form, and won't be by the time the reports on incentives are due to the President, it is unclear what "adopting the framework" means in pragmatic terms. The only cyber incidents specifically identified in the EO are the catastrophic events alluded to above. As mentioned, if the framework is designed to address this threat, the incentives will need to be extremely powerful, especially since the likelihood of the threat is "remote." If, on the other hand, the framework is designed to simply encourage good cyber hygiene and address the gap between commercial security needs and national security needs discussed above, the incentives can be of a more moderate nature. However, even in this instance, one needs to be careful not to take too much solace from studies suggesting that a large portion of cyber events could have been prevented had best practices and standards been utilized. While this research, such as the post facto analysis of the Verizon-Secret Service studies, may well be accurate, the fact that standards/practices would have prevented the successful attacks have definite limitations. Advanced attackers will often use simple methods of attacks if such methods achieve the attackers' ends(such as in the 80-90% of cases often cited). However, they will also elevate their attack methods in cases where they are mitigated by basic defense. As such, the fact that a practice might have prevented the exact attack that occurred is not necessarily proof that had that method actually been used the attack would not have succeeded since we don't know whether the attacker would have simply used a more potently attack in the face of basic defenses. Finally, if the system envisioned by the EO is truly to be risk-based, the goals cannot legitimately be "all of the above." The fundamental principle of risk management is setting clear goals and making investments based on realistic ability to meet these goals. What risk management translates into in a pragmatic sense is an answer to the question "How much security do you want to buy? Or, in this case, do you want to incentivize?" Once the framework makes the goals clear, the incentive structure can be much better defined.
7. ***Principles of Effective Incentives***
    - The key issue in judging whether or not to deploy an incentive is will the incentive deployment be sufficient to meet the stated goals. As was clearly described at the workshop, some proposed incentives such as positive recognition are generally not viewed as actual incentives by the private sector (and are even possibly something to be avoided, as it may increase the likelihood of being targeted), while other incentives that have been proposed attract little interest, as they are unlikely to even be utilized. One oft cited example is the protection from punitive damages offered in some previous legislation, as the general assumption was that actual damages would be so overwhelming in these cases as to make this supposed incentive moot.

      The Internet Security Alliance has suggested five recommended criteria for effective incentives:

        1. Incentives must be powerful enough to affect corporate investment behavior;
        2. Incentives must be calibrated to match the additional investment required to adopt EO framework/other goals;

3. Incentives vary not just from sector to sector, but business to business, and, thus, a menu of incentives is needed that allow individual entities to choose what incentive will justify presumably additional cyber security investment;
4. Regulations that do not include full cost recovery are not a substitute for incentives because they are not economically sustainable; and
5. Costs incurred to increase cyber security, and not compensated through incentives, will invariably come from consumers paying more or reduced attractiveness in critical infrastructure investment – there is no free lunch.

8. Incentives Need to Be Applied At the Corporate Level, Not the Sector Level

- Even within a sector, one-size-fits-all does not apply, as even relatively homogenous sectors often have substantial differences at the owner/operator level. Incentives must be applied at the corporate level to be effective, and only each individual corporate entity is in a position to evaluate what policies and incentives work best for them. Therefore, there should be a menu of market incentives available for corporations that elect voluntary adoption of effective standards and practices.

9. Even Regulated Sectors May Still Use Incentive Programs Modeled on Current Programs Designed to Achieve Other Pro-Social Ends, But Now Applied to Cyber Security

- For regulated companies that voluntarily adopt the Framework, mechanisms for cost-recovery akin to those utilized by FERC could be used:
  - One example is the [FERC] policy statement addressing Extraordinary Expenditures Necessary to Safeguard National Energy Supplies (http://www.iso-ne.com/committees/comm_wkgrps/trans_comm/tariff_comm/mtrls/2002/oct102002/A4_1466800.pdf). In this policy statement, FERC acknowledged that "electric, gas, and oil companies may need to adopt new procedures, update existing procedures, and install facilities to further safeguard their electric power transmission grid and gas and oil pipeline systems." FERC stated that it would permit companies to propose a separate rate recovery mechanism.
    - Once such mechanism is a surcharge to currently existing rates
    - In accordance with this policy, FERC has approved separate surcharges requested by certain offshore natural gas pipelines to recover the costs of excessive hurricane damage.
    - FERC has granted certain individual pipelines' requests to revise their tariffs to reflect that they may be required to reduce service to firm customers as a result of temporary outages required to comply with pipeline safety requirements imposed by PHMSA
    - See Shell: http://www.ferc.gov/EventCalendar/Files/20040227171713-IS04-171-000.pdf; and Mid-America Pipeline Company: http://www.ferc.gov/EventCalendar/Files/20060629171306-IS06-348-000.pdf).
  - Other FERC incentive mechanisms were authorized and required under the Energy Policy Act of 2005 (EPACT) and later amendments. See (http://www.gpo.gov/fdsys/pkg/PLAW-109publ58/pdf/PLAW-109publ58.pdf).
    - Under EPACT Congress required the FERC to establish, by rule, incentive based rate treatments for the transmission of electric energy in interstate commerce by public utilities for the purpose of ensuring reliability and reducing the cost of delivered power by reducing transmission congestion.

- Specifically, among other things, Congress required the Commission to provide a return on equity that attracts new investment in transmission facilities (including related transmission technologies); to encourage deployment of transmission technologies and other measures to increase the capacity and efficiency of existing transmission facilities and improve the operation of the facilities; and to allow the recovery of all prudently incurred costs necessary to comply with mandatory reliability standards.
- In response, the Commission issued a rulemaking entitled Promoting Transmission through Pricing Reform. After several years of experience with that rule, the Commission recently issued a Policy Statement providing clarification and guidance. Generally, developers of transmission facilities can request that the Commission provide them with incentives, including an incentive Return on Equity (ROE) to develop a proposed project that is designed to improve reliability or relieve congestion.
- Applicants may also request "Risk Reducing Incentives," such as recovery of 100 percent (rather than 50%) of Construction Work in Progress (CWIP), recovery of 100 percent of pre-commercial costs as an expense or as a regulatory asset, and recovery of 100 percent of prudently incurred costs of transmission facilities that are abandoned for reasons beyond the applicant's control. The Commission stated that it expects incentives applicants to first examine the use of risk-reducing incentives before seeking an incentive ROE based on a project's risks and challenges.

▪ Other EPACT Incentive provisions include:
- Under an amendment in the American Recovery and Reinvestment Act of 2009, Section 406, the Energy Policy Act of 2005 authorizes loan guarantees for innovative technologies that avoid greenhouse gases, which might include advanced nuclear reactor designs, such as pebble bed modular reactors (PBMRs) as well as carbon capture and storage and renewable energy;
- it seeks to increase coal as an energy source while also reducing air pollution, through authorizing $200 million annually for clean coal initiatives, repealing the current 160-acre (0.65 km2) cap on coal leases, allowing the advanced payment of royalties from coal mines and requiring an assessment of coal resources on federal lands that are not national parks;
- it authorizes subsidies for wind and other alternative energy producers, including those utilizing wave and tidal power;
- it authorizes $50 million annually over the life of the law for biomass grants;
- it includes provisions aimed at making geothermal energy more competitive with fossil fuels in generating electricity;
- it requires the Department of Energy to designate National Interest Electric Transmission Corridors where there are significant transmission limitations adversely affecting the public (the Federal Energy Regulatory

Commission may authorize federal permits for transmission projects in these regions);

- it authorizes the Department of the Interior to grant leases for activity that involves the production, transportation or transmission of energy on the Outer Continental Shelf lands from sources other than gas and oil (Section 388);
- it provides a multitude of tax breaks by industry and for those individuals making energy conservation improvements to their homes;
- it provides incentives to companies to drill for oil in the Gulf of Mexico;
- it exempts oil and gas producers from certain requirements of the Safe Drinking Water Act;
- it sets federal reliability standards regulating the electrical grid (done in response to the 2003 North America blackout);
- it extends the Price-Anderson Nuclear Industries Indemnity Act through 2025;
- it authorizes cost-overrun support of up to $2 billion total for up to six new nuclear power plants;
- it authorizes production tax credit of up to $125 million total a year, estimated at 1.8 US¢/kWh during the first eight years of operation for the first 6.000 MW of capacity, consistent with renewable; and
- it authorizes loan guarantees of up to 80% of project cost to be repaid within 30 years or 90% of the project's life.

10. Removing Barriers Can Be As Effective As Granting New Benefits

- Incentives can equate with a removal of barriers. For example, while it is reasonable for a private entity to have to demonstrate adoption of a particular standard to qualify for an incentive benefit, the costs of the compliance regime can substantially mitigate the benefit of the incentive. There are numerous, different, and sometimes-conflicting, audit and compliance regimes, for example, that a single entity needs to adhere to. While the EO does call for streamlining these regimes, a further step could be to offer the streamlined process as a benefit for good actors. Forbearing from regulation, based on demonstrated adherence to an approved regime, can provide an ongoing incentive for entities to continually upgrade their security in order to save the tremendous costs of multiple redundant auditing regimes.

11. Preferential Treatment in Government Process for Good Actors Can Be A Powerful Incentive

- For technologies that would advance cyber security and adherence to the Framework, rapid time to market could be both beneficial to those that adopt them and is often required for businesses that choose to innovate them. However, there are several barriers to Fast Tracking and thus innovation itself: (1) the patent system is slow, and (2) companies that produce such technologies fear lawsuits unless they have more time for testing. In order to remove these barriers, cyber security technologies could receive preferential treatment and a streamlined patent process and that those products that are Fast Tracked could receive liability protections, such as damage restrictions, partial indemnity or immunity, etc. Other example of preferential treatment that could, be offers, or used as a model for great voluntary adoption of approved secure standards and practices could be:
    - Companies that voluntarily adopt the Framework could also be eligible for preferential treatment in the form of:

- Take-off and landing preferences for the aviation industry**;**
- Security Clearance preferences so that those that voluntarily adopt the Framework are moved to the front of the line**;**
- Expedited patent review so that those that voluntarily adopt the Framework are moved to the head of the patent review line**;**
- Federal-permitting preferences so that those that have some type of permit review would have their permit reviews expedited if they adopt the Framework

▪ Companies that voluntarily adopt the Framework could also receive partial indemnity from the Government should they purchase cyber insurance and should a cyber event occur.

12. The SAFETY Act Could Be Modified to be a "Cyber SAFETY Act"

o The current SAFETY Act is tasked with determining whether certain products and services help mitigate against terrorist attacks. In making this determination, the Office judges these products and services on a sliding scale (or tiered level) of effectiveness. Those that meet a higher threshold receive a "certification" determination, whereas those that meet a somewhat lower threshold receive a "designation" determination. Those that receive the higher "certification" level under the SAFETY Act also receive a higher level of benefits/incentives. This idea of evaluating measures and technologies on a sliding scale of effectiveness, with more effective measures/technologies receiving higher value incentives, is something that could be emulated with respect to adherence to global standards and/or the Framework and Incentives program.

While the SAFETY Act has a broad definition as to what measures/technologies could receive designation or certification, the definition is nonetheless captioned as "qualified anti-terrorist technologies." Such terminology has resulted in minimal use of the SAFETY Act for cybersecurity technologies because companies fear legal challenges down the road as to whether DHS has the authority under the law to designate or certify such technologies. To remove this doubt, the SAFETY Act could be modified so that what qualifies is not only "anti-terrorist technologies," but explicitly "cybersecurity technologies" as well. Both the definition of cybersecurity technologies and cyber incident should be as broad as that of what constitutes terrorism and anti-terrorist technologies under the act.

o In terms of incentives, the incentives in the SAFETY Act could also be applied in a cybersecurity context. Those that adhere to the Framework could receive the litigation benefits of case consolidation and transfer to federal court as described in the SAFETY Act. Other incentives include dismissal of third party claims, damage limitations, promotion of insurance in that insurance purchase is coupled with partial indemnity.

▪ For more on the SAFETY Act, see https://www.safetyact.gov/pages/homepages/Home.do

13. Government Should Streamline Its Own Process

o If the government truly wants people to adopt and adhere to a Federal Framework, it should tie adoption to the framework with preemption of other federal agency regulations and audits as well as state and local laws, regulations, frameworks, etc., whose purpose is similarly to raise cybersecurity. It is unreasonable and counterproductive for government to expect the private sector to modernize its

systems, but refuse to modernize its own governmental processes due to purely political considerations.

14. Preemption Can Be An Effective Mode of Providing Incentives

- Businesses processes that are determined to be effective should be certified under the Framework as effective, and with such a certification, those companies that utilize them should have some level of liability protection or other incentives. This liability protection can be of varying levels (no punitive damages, no actual or punitive, altering the burden of proof, providing an affirmative Defense) based on the relative effectiveness rating of the framework adopted (this assumes multiple frameworks are available as advocated elsewhere).

15. Stimulating the Private Insurance Market Could Result In A Productive Private Sector Incentive Program

- Insurance is one of the most successful tools currently existing for promoting pro-social behavior, such as in health care or automotive and building safety. A robust cyber insurance system could have multiple positive effects. Such a system could generate a private sector system of continually evolving effective best practices motivated by the insurance industry's desire to prevent cyber incidents and, thus, reduce claims. Once in place, such a system could provide a market driven set of economic motivators to adopt improved cyber security practices in order to achieve premium discounts, as is routinely done in car and other insurance markets. Finally, insurance could provide a market-based system of compliance, as insurance carriers would have ample motivation to assure the practices they had deemed necessary to qualify for policies were actually being adopted.
- Unfortunately, the cyber insurance market, aside from recent growth in "third-party" policies (i.e., to pay costs associated from public notices stemming from mandated breach notification laws), has experienced sluggish growth. Carriers seem to be reluctant to offer policies covering the sorts of events specified in the EO, and a lack of generally available actuarial data is often cited as a reason. Presumably, the lack of data leads carriers to set prices at maximum risk rates, thus deterring entities from buying the policies.
- In order to foster an insurance market, the Government could acknowledge the de facto reality that it would be the insurer of last resort should a cyber-Katrina/wide-ranging nation-state attack occur. A revolving fund could be established, similar to those previously used to stimulate crop and flood insurance markets, which could then be drawn down as more insurers enter the market and replace that fund with private money generated from policies sold. Theoretically, with the revolving fund providing assurance of the ability to survive a catastrophic cyber event, more carriers would enter the market, driving down the costs of policies and generating additional sales. This would put further pressure on rates, and a virtuous cycle of sales and protective measures would ensue.

16. Federal Acquisition Policy Could be Altered to Motivate Improved Cyber Security

- GSA-DOD Federal Acquisition recommendations currently under consideration, include:
  - Entire federal acquisition spend should be (1) categorized, (2) assessed for cybersecurity risk, and (3) prioritized according to risk, essential functions and agency mission;
  - Agencies should require cybersecurity assessment for all acquisitions early in the requirements definition phase;

        - Acquisitions should have cybersecurity concurrence / approval prior to issuing the solicitation and again prior to contract award;
        - Acquisitions should have cybersecurity approval/review of contractor performance during contract administration; and
        - A common lexicon should be developed for use in acquisitions related to cybersecurity.
            - A common, but role-focused, training program should be developed for acquisition stakeholders.
    - Other proposals worthy of consideration are:
        - A federal acquisition incentive could include relief from certain other FAR regulations that might be overly burdensome and not germane for the supplied product or service if an entity adopts the Framework.
        - Include indemnification or partial indemnification for claims arising from supplied products.
        - Federal acquisition preferences, such as those utilized in the minority-owned business, woman-owned small business, and veteran-owned small business programs as described in The Veterans Benefit Act of 2003; Small Business: 15 USC 633 et seq; Women and Minorities: 15 USC 637; the Office of Federal Procurement Policy Act of 1974 (Pub. L. 93-400).
        - Federal acquisition rebates as utilized in the "Indian Incentive Program" - http://www.acq.osd.mil/osbp/sb/programs/iip/
            - The Indian Incentive Program (IIP) is a congressionally sponsored program that provides a 5% rebate back to the prime contractor on the total amount subcontracted to an Indian-Owned Economic Enterprise or Indian Organization, in accordance with DFARS Clause 252.226-7001. Department of Defense (DoD) prime contractors, regardless of size of contract, that contain the above referenced clause(s) are eligible for incentive payments. DoD prime contractors with a contract of $500,000.00 or more that contain the above referenced clause(s) are eligible for incentive payments.

17. Other Incentives

- Similarly, the Government could fund or enable research into the cost benefits of reducing botnet, spam, malware, etc., as is needed and described in the latest CSRIC report: http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf (CSRIC, p.52).
- For companies that are innovators, adherence to the Framework could result in access to innovation clusters or an innovation forum.
    - It could also result in future R&D grants.
- Such companies could also have access to certain marketing benefits/brand recognition, while others that feel as if it would make their corporations a target could decline.
- Grants could be given to various Information Sharing and Analysis Centers so that their maturity levels could be raised.

18. Other Existing Incentive Models That Could Be Adapted for Cyber Security

- In addition to the above incentives, the following incentives that have been used in other areas of the economy could be explored as models and for possible adaptation to cybersecurity:

- Under the Digital Millennium Copyright Act of 1998, Internet Serve Provider's legal exposure in terms of copyright infringement was clarified so that ISPs would provide internet services. Namely, the Act provided the ISPs with safe harbor from liability for their users' actions with respect to copyright infringement provided that the ISPs adhered to certain other requirements.
- To motivate Internet and Communications providers to supply wireless broadband to areas where it would not be business justifiable/profitable (e.g., rural areas), the Obama Administration issued policy statements in 2010 and 211, entitled, Obama "Unleashing the Wireless Broadband Revolution" and the "National Wireless Initiative," respectively. Together these documents urged both the U.S. Congress the DoC's National Telecommunications and Information Administration to "adopt proposals to improve the process for reassigning spectrum encumbered by Federal users to private use, grant authority for the FCC to hold incentive auctions, create governance structures and channel auction proceeds to manage the deployment and operation of a nationwide interoperable public safety broadband network, and spur innovation in wireless services by both providing for unlicensed access to wireless spectrum and funding critical research and development."
- In order to motivate the business community to hire those that are longer term unemployed – those that have been unemployed for at least 60 days – the President and Congress signed into law the "Hiring Incentives to Restore Employment (HIRE) Act." This law cut employer taxes for those businesses that hired such individuals. More specifically, employers that hired such individuals in 2010 qualified for a 6.2-percent payroll tax incentive, in effect exempting them from their share of Social Security taxes on wages paid to these workers after March 18, 2010 as well as $1000 business tax credit for year 2011 if the workers were retained for at least a year.
- In order to provide assistance to small businesses, those that have been service disabled, and those that have been historically discriminated against (i.e., women and minorities), the federal government has set up federal procurement programs to aid these groups in obtaining federal procurement contracts: The Veterans Benefit Act of 2003; Small Business: 15 USC 633 et seq; Women and Minorities: 15 USC 637; the Office of Federal Procurement Policy Act of 1974 (Pub. L. 93-400).
- Under the FAA Modernization and Reform Act of 2012, Secretary of Transportation is granted the authority to establish an "equipage incentive program" to equip US registered aircraft with NextGen technologies and capabilities. While the FAA act mentions the establishment of a "loan guarantee program," other incentives that are being considered include preferential take-off and landings for those equipped with NextGen technologies.
- In order to encourage health care providers to move to electronic based health records so that the records will be more readily available to patients and decrease paper related costs for federal and state agencies, the government has enacted both HIPAA/HITECH and subsequent regulations. Under these authorities, the government has been providing direct monetary incentives to eligible healthcare professionals that move to e-health records within a specific timeframe and that meet certain "meaningful use" requirements. For eligible professionals providing healthcare to medicare patients, payouts can reach as

high as $44,000 per provider, released over a 5 yr period. For Medicaid, the incentive maximum per provider is $63,750.

- Effectiveness: Since the program started, the AMA has reported that over 125,000 healthcare providers have opted into the incentive based program.
- Authority: HIPAA/HITECH and HIPAA/HITECH Regulations 42 CFR Parts 412, 413, 422 et al

- Under the Orphan Drug Act (ODA) of 1983 (and subsequent amendments), "drugs, vaccines, and diagnostic agents" qualify for orphan status if they are intended to treat a disease affecting less than 200,000 American citizens. In order to encourage the development of drugs for such orphan diseases, the ODA included a number of incentives including seven-year market exclusivity for companies that developed orphan drug, tax credits equal to half of the development costs (later changed to a fifteen-year carry-forward provision and a three-year carry-back that can be applied in profitable year), grants for drug development, fast-track approvals of drugs indicated for rare diseases, and expanded access to the Investigational New Drug Program. The law was also later amended to waive FDA user fees.
    - Effectiveness: In the USA, from January 1983 to June 2004, a total of 1,129 different orphan drug designations have been granted by the Office of Orphan Products Development (OOPD) and 249 orphan drugs have received marketing authorization. In contrast, the decade prior to 1983 saw fewer than ten such products come to market. In 2010, Pfizer established a division to focus specifically on the development of orphan drugs as other large pharmaceutical companies focused greater efforts on the orphan drug research.
- In order to reduce the amount of fatalities at railroad and road intersections/crossings, the Federal government enacted a program whereby it would fund the States to fix selected dangerous crossings that were self-identified by private sector owners and operators as dangerous. In order to assure private sector cooperation in identifying those crossings, the Federal government provided that the identifying documentation, etc., produced by the private sector would not be discoverable in either State or Federal litigation proceedings.
    - Effectiveness: From 1973 to 2005, approximately $4B has been spent on 23 U.S.C. 130 program grade crossings. Program has been credited with dropping fatality rates at grade crossings by 70%. (Texas Transportation Institute Report).
    - Authority: Highway Safety Acts and Surface Transportation Assistance Acts (aka the 23 U.S.C. 130 Program).
- When it became apparent that the private sector was refraining from entering the nuclear power generating business because companies could not obtain insurance to cover possible incident expenses at acceptable levels, the Federal Govt enacted the Price-Anderson Nuclear Industries Indemnity Act wherein the Govt provided that if nuclear power companies purchased the highest level of insurance available, it would cover litigation costs beyond that of the insurance purchased using a revolving fund of user/generator fees. The Act also provided that companies were exempt from punitive damages and would receive

litigation incentives, such as the required consolidation of cases and transfer to a single federal court.

- Effectiveness: Following its enactment, private sector companies entered into nuclear power generation.

- In order to encourage businesses to remediate and develop hazardous waste sites, to reduce carbon emissions, acid rain, etc., the U.S. Congress and EPA have developed a series of different programs wherein good actors would receive certain incentives described at left.
    - Effectiveness: According to the EPA report cited below, "it is clear that economic incentives do provide the opportunity to achieve any given level of pollution control with substantial cost savings…At least 40 studies based on computer modeling of different scenarios for controlling pollution show what economic incentives should be more cost-effective than traditional regulations. One study (ICF, 1989) estimated that allowance trading in EPA's acid rain program could result in savings to effected utilities of $700 to $800 million per year over the long term. The actual cost savings now are believed to be at least twice this amount." (EPA Report, pp.ix-x).
    - For Greater Detail: See the EPA's January 2001 Report, entitled "The United States Experience with Economic Incentives for Protecting the Environment": http://yosemite.epa.gov/ee/epa/eerm.nsf/vwan/ee-0216b-13.pdf/$file/ee-0216b-13.pdf
        - Incentive Types discussed:
            - Limited Liability for Owners of "Brownfields" that work to remediate hazardous sites;
            - Choice of Hazardous Site Remediation Levels;
            - Streamlined Permitting;
            - Marketable Permits; and
            - Subsidies, Grants, and Tax Exemptions.

A National Model for Cyber Protection
Through Disrupting Attacker Command and Control Channels

Jeff Brown, CISO, Raytheon Company

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 long survive 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.

Raytheon believes the best way to address this new reality is to recognize that attackers will get into your network and expand our defensive actions to detect, disrupt, and deny attacker's command and control (C2) communications back out to the network. It is an acknowledgement of the fact that there are fewer, or perhaps 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. Raytheon has had success with this strategy, 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, both of which we are pursuing in Raytheon. The first is to make a considerable investment in traffic analysis and analytical methods to detect the malicious outbound traffic in a network. We 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.

It is in the collaboration realm that Raytheon believes there is an opportunity for a national scale effort that can turn collective effort to our advantage in the cyber battle. 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.

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 outbound 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 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.

This document, then, proposes a model for standing up a National Cyber Threat Protection Service to implement a C2 disruption strategy. It will describe the process, key relationships, and responsibilities of the participants and the incentives for each community of interest. This is a voluntary model. Within all the communities described below, not everyone has to participate for the model to be effective. The more the better, but once the process includes a critical mass, the benefits will quickly accrue to a wide swath of both the public and private sector.

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. **A National Cyber Threat Response Center (NCTRC)** which 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, 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 deconflict 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, Critical Infrastructure Providers, and Government

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 up front 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 reclama or deconfliction 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.