The Internet Security Alliance

Response to the

National Institute of Standards and Technology's Feb. 26, 2013 Request for Information: "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

April 8, 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.

Current Risk Management Practices:
NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

"Current Risk Management Practices" Section Questions and ISA Responses:

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

ISA Response:

A. <u>Research Consistently Shows the Biggest Challenges are Economic.</u>

There has been a fair amount of research on the question of what is the greatest challenge to the improvement of cyber security, and the data points in one direction: the single biggest obstacle to cyber security improvement across critical infrastructure (and non-critical infrastructure) is cost. Among the empirical research that has documented this fact are the large-scale studies conducted by PricewaterhouseCoopers, CIO Magazine, and CSIS & McAfee.[1],[2],[3]

Using an entirely different methodology, in 2009, the President tasked Melissa Hathaway together with members of the White House and the National Security Council to do a comprehensive assessment of the roles of both the public and private sectors in cyber security, which reported that "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost or complexity."[4]

Accordingly, the empirical finding that cost is the greatest challenge to securing critical cyber systems demands that a greater analysis of the economics of cyber security be completed. When advanced analyses have been done, they indicate that the issues that must be addressed to develop a sustainably secure cyber system go well beyond the laudable (but ultimately insufficient) attempt to promulgate a framework of standards as a solution to our cyber threats.

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

[2] CIO Magazine. "Business Partners with Shoddy Security; Cloud Providers with Dubious Risk Controls; What's a CIO to Do?" Oct. 2010.

[3] McAfee and Center for Strategic & International Studies. "In the Crossfire: Critical Infrastructure in the Age of Cyber War." 2010.

[4] Executive Office of the President. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." Rep. The White House, May 2009. Web. <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. P.31.

B. Misaligned Incentives for Cyber Security Are A Bigger Problem Than A Lack of Standards.

As will be described exhaustively in the filings, there is no shortage of developed and empirically tested standards and practices. Rather than a lack of standards, the greater problem that exists is a misalignment of incentives for increased cyber security or cyber hygiene.

According to one seminal report's findings, since "distributed systems are assembled from machines belonging to principals with divergent interests, we find that incentives [become] as important as technical design . . . security failure is caused at least as often by bad incentives as by bad design."[5]

In the early days of cyber security most attacks were benign with many expressly designed to show off expertise. That is not the case with the attacks against critical infrastructure that could cause a regional or national catastrophe, the prevention of which is the expressed Presidential directive for the NIST Framework. Modern cyber attacks (i.e., *advanced persistent threats*) are designed to be stealthy. Such threats can be directed at business and political targets over a prolonged duration of operations.[6]

Those that levy such attacks know that the incentives calculus favors them. Indeed, virtually all the economic incentives with respect to cyber security favor the attackers. Cyber attacks have become easy as well as cheap, which also can be out-sourced inexpensively through the Internet. In addition, attacks can be extremely profitable, with the estimates of annual theft ranging in the billions of dollars. Moreover, the chances of getting caught are slim, with estimates indicating that less than two percent of cyber criminals are successfully prosecuted.[7]

By contrast, cyber defense has numerous economic disincentives with the defenders usually lagging a generation behind the attackers. And the perimeter to be defended is virtually limitless. Return on investment, a critical calculus in the private sector where firms are obligated to be profitable, is difficult to demonstrate. It is complicated by mandated compliance regimes that are counterproductive because they can drain resources without improving security. Even with a return on investment, success requires preventing something from happening, which is almost impossible to measure.

As long as the economic equation for cyber security remains unbalanced, standards espoused by a framework will not remedy the problem. The incentives to attack will virtually guarantee continued successful attacks by continually more sophisticated attackers.

With respect to those that are subject to the attack, there are also incentive misalignments. Like the misalignments discussed above, these too must be redressed. More specifically, in the cyber security world, negligent or culpable parties are not necessarily penalized for their actions. A review of the literature on information security similarly discovered that jurists "have long known that liability should be assigned to the part that can best manage the risk. Yet everywhere we look we see online risk allocated poorly . . . people who connect insecure machines to the Internet do not bear the full

---

[5] Anderson, Ross, and Tyler Moore, "The Economics of Information Security: A Survey and Open Questions," *Science* 314 (October 27, 2006): 1.

[6] "Advanced Persistent Threats (APT)" Rep. Damballa, 2010. Web. <http://www.damballa.com/knowledge/advanced-persistent-threats.php>.

[7] Regoli, Robert M., and John D. Hewitt, *Exploring Criminal Justice: The Essentials* (Sudbury, MA: Jones and Bartlett Publishers, 2010), 378.

consequences of their actions ...[and] developers are not compensated for costly efforts to strengthen their code."[8]

One obvious example is personal liability associated with lost credit cards. If one engages in risky behavior that results in credit card theft and thousands of dollars being charged against the accounts, what is the personal liability? In the United States it is a minimal amount of fifty dollars. Banks on the other hand, which are not culpable for such losses, bear most of the cost. Moreover, banks pass on the cost to their customers in transaction fees and interest rates.

A similar complication arises in the theft of corporate intellectual property. The problem of interdependent risk occurs when corporate information technology infrastructure is connected to other entities in such a way that it leads to failures elsewhere.[9] This risk will lead firms to under-invest in security technology and cyber insurance. For example, assume that a rogue state or criminals attempt to steal intellectual property from a high-value target. Accessing the target may be difficult because of substantial investments made to prevent unauthorized entry to its system. However, the same information may be found on less protected networks belonging to a partner or contractor. Thus the attack could be mounted against a weaker element in the system.

In such instances, the edge entity on the point of attack may not suffer any economic impact and has little incentive to prevent similar attacks. On the other hand, the ultimate target would not only suffer potentially severe impacts, it also reveals that investments are being undermined by an entity on the edge at the point of the attack. Research has confirmed the security downside of such interdependency: "Further externalities can be found when we analyze security investment, as protection often depends on the efforts of many principals. Budgets generally depend on the manner in which individuals' investments translate into outcomes, but the impact of security investment often depends not only on the investor's own decisions but also the decisions of others. ...Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail."[10]

C. Cyber Security Needs to be Analyzed and Understand from a Broader Systems Perspective.

While the economics of cyber security is rarely mentioned in public policy discussions, when it is, unfortunately, the focus of the conversation centers entirely on the potential economic impacts of a successful attack. Regrettably, the sole question that is usually asked is: "if enterprises are afraid of losing millions of dollars worth of corporate data, why don't they invest in standards and practices that would adequately assure cyber security?"

The thought process and analysis underlying this question misses the mark in three critical respects:

First, the private sector is already investing heavily in cyber security. In fact, 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.;

---

[8] Anderson and Moore, "Information Security," 2-3.

[9] See Larry Clinton, "The Internet Security Alliance answer to the Department of Commerce Notice of Inquiry: Cybersecurity, Innovation and the Internet Economy" (Arlington, VA: Internet Security Alliance, September 20, 2010), 9.

[10] Anderson and Moore, "Information Security," 1, 4.

governance and control activities, such as traffic monitoring, compliance, and training; security management outsourcing; and securing industrial control systems.[11] 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.[12] 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.[13] This was the complete requested budget, inclusive of FEMA, TSA, ICE, etc.

This massive increase in private sector spending – the doubling to $80 billion within a five year span – has only exacerbated the cost tensions that have been documented in the referenced studies. While many critics inexplicably and unjustifiably claim private sector negligence and a lack of concern for cyber security, such a claim is false. Rather, must make decisions that are business justifiable as they are legally mandated to do and are caught in the vice of misaligned incentives.

This leads to the second, and often ignored, critical factor in understanding the economics of cyber security: namely, that private sector cyber security investment needs to be appreciated on a company by company basis. Cyber security investments are not done by sector, but by each individual company, which also face the legal constraint of maximizing their shareholder value.[14],[15] So while overall the amount of cyber security investment has increased dramatically in the past few years, this level of spending does not necessarily translate to every single company. For example, according to PwC's most recent annual Global Information Security Survey, only 45% of those polled expected an increase in security budgets, while 28% reported having to defer planned-for security projects.[16]

Third and finally, focusing on end system security features (and not the full investment system industry faces), to address the long-term speculative downside of potential cyber events fails to appreciate the numerous near-term, easily documented economic incentives to deploy technologies and business processes that a leave an organization less secure. In many cases, making these less secure business investments is essential to the economic well-being of the company, which is the legal mandate of Boards of Directors and senior management.

Moreover, when developing a program that the government seeks to enforce either through incentives or regulatory mandates, as suggested in the Executive Order, NIST must take into account not only the incremental cost of individual security measures, but the overall impact of information system investment strategy on the economics of the enterprise as well as the subsequent impact on the overall economy in terms of innovation, investment and job development.

---

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

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

[13] 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>.

[14] Dodge v. Ford Motor Co., 170 N.W. 668 (Mich.1919).

[15] Carlton Investments v. TLC Beatrice International Holding, Inc., 1997 Del. Ch. LEXIS 86, 45 (ct. of Chancery, New Castle May 30, 1997).

[16] PricewaterhouseCoopers. "PwC 2013 Global State of Information Security Survey" Rep. 2013. Web. <http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf>.

This means that NIST should also address (or at least understand) that there are systemic incentives to be insecure or to be "cyber risky." Addressing these systemic incentives to be "cyber risky" is a far greater challenge than cataloging and encouraging standards and practices, as beneficial as that may be.

Indeed, the number of examples of these systemic economic incentives to be insecure is legion. The adoption of unified communications (UC) platforms, such as voice-over-Internet protocol (VoIP) 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."[17]

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 benefits ranging from cost savings and efficiencies.[18] 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.[19]

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

ISA Response:
See ISA's Response to Question 1 above.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

ISA Response:
ISA membership consists of some of the most cyber sophisticated organizations. Many ISA members utilize an enterprise-wide, risk-based approach to handling cyber security risk. Discussed more fully below in ISA Response to Question 4, 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

[17] 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 >.

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

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

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.

4. Where do organizations locate their cybersecurity risk management program/office?

ISA Response:
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.[20]

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).[21]

The 2008 Carnegie Mellon University-CyLab study also provided alarming details about the state and structure of enterprise risk management of cyber security.[22] The study pointed out that:

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

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" and "The Financial Management of Cyber Risk: An Implementation Framework for CFOs," 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

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

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

[22] Carnegie Mellon CyLab. "Governance of Enterprise Security Study: CyLab 2008 Report." Rep. CMU CyLab, December 2008.

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-wide framework and was released in 2012. 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.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

ISA Response:

A. <u>The Private Sector and Government Assess Cyber Security Risk Differently Due to Their Legally Defined Responsibilities.</u>

As well as understanding relationships between business economics and cyber security, policy makers must be mindful that the responsibilities of public and private entities are not the same. The role of the federal government enshrined in the Constitution is providing "for the common defense,"[23] while the role of industry, which is supported by nearly a hundred years of case law, involves maximizing shareholder value.[24],[25] These traditional roles produce significantly different approaches to making critical decisions on cyber security risk assessment.

Although no one wants to be the victim of attacks, as compared to the Government, industry may have a higher risk tolerance (inclusive of cyber risk). For example, it is common for retailers to accept that a

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

[24] Dodge v. Ford Motor Co., 170 N.W. 668 (Mich.1919).

[25] Carlton Investments v. TLC Beatrice International Holding, Inc., 1997 Del. Ch. LEXIS 86, 45 (ct. of Chancery, New Castle May 30, 1997).

certain amount of their inventory will "walk out the back door" every month. Some businesses tolerate this situation, however, because the expense of hiring guards, installing cameras, etc., may exceed the value of the merchandise being stolen and their lower level of security is written off as a cost of doing business.

Because government is charged with defending its citizens and not concerned with profit margins, it may have a much lower risk tolerance. Increased regulation will not overcome this risk tolerance/risk assessment gap or "delta." Any regulation or framework of standards would surely be outdated by the time they are issued. Moreover, with respect to this delta, Ponemon Institute-Bloomberg Government has estimated to reach an acceptable, not an ideal, level of cyber security, an additional 91% annual spending increase would be needed by the critical infrastructure[26], which is already spending over $80 billion annually.[27] Accordingly, to address this gap, Government should/will have to deploy incentives powerful enough for organizations to match this higher level of security.

B. How Private Sector Organizations Generally Define Cyber Security and Assess Cyber Security Risk.

Against this context of aligned, but distinct, Government-private sector cyber risk definitions and metrics, ISA work has revealed that its membership – a group of cyber sophisticated organizations – generally define cyber security risk as a component of overall enterprise risk. ISA members that have shared their risk management approaches typically consider this particular risk – cyber risk – alongside other risks, such as natural disasters, supply chain risks, human resources risks, espionage, etc. One ISA organization defined technology risk (i.e., cyber risk) as "business risk associated with the use, ownership, operation, involvement, influence and adoption of information technologies within an enterprise."

Identified risks are then evaluated holistically, with the organization determining how the risk (if realized) could affect its operations, finances, and reputation. Following this identification and evaluation, ISA organizations then typically "heatmap" and prioritize the risks based on the risk's probability of realization and impact if realized, with dollar amounts assigned for potential operational, financial, and reputational harms. Depending on the nature of the risk, its prioritization placement, its probability of realization, and its potential impact, businesses then pick among the traditional strategies of avoid, reduce through mitigation, transfer, or accept, depending on their own business plans, the strategy's cost-justifiability, the company's risk tolerance levels, and/or resource availability. This decision is made in the context described above and within the business's legal mandate to maximize shareholder value.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

ISA Response:
See ISA's Response to Question 5 above.

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

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

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

ISA Response:

The December 2011 GAO Report, entitled, "Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote its Use," and referenced in this NIST request for information, notes: "In September 2008, we (GAO) reported that there are at least 34 federal laws, regulations, and mandatory standards that pertain to securing privately owned IT systems and data in our nation's critical infrastructure sectors and each of the 34 federal legal requirements… See GAO-08-1075R."[28] This 2008 Report, entitled, "Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors," provides these 34 requirements. However, this report also notes that there are more than these 34 requirements, that in calculating this number, the GAO did not take into account the authorizing laws for such regulations, which, of course, provides authority for even further cyber security regulation since this report was issued in 2008. These specific regulatory requirements and the critical infrastructure segments that they pertain to can be found on pp.49-72 of the report.[29]

Since 2008, regulatory interest with respect to cyber security has only grown. Moreover, certain sectors, such as the energy sector, are not only subject to federal regulators, but State and local regulators as well. With respect to data privacy, at the State level, there are at least forty-six States, as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, that have enacted legislation requiring notification of security breaches involving personal information.[30] Additionally, each State and the Federal government have enacted Unfair and Deceptive Acts and Practices (UDAP) legislation[31], and, increasingly, these statutes are being utilized in the context of cyber security.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

---

[28] Government Accountability Office. "Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote its Use." Rep. Washington, D.C. Dec. 2011, GAO-12-92, p.24. Web. <http://www.gao.gov/assets/590/587529.pdf>.

[29] Government Accountability Office. "Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors." Rep. Washington, D.C. July 2008, GAO-08-1075R. Web. <http://www.gao.gov/assets/100/95747.pdf>.

[30] National Conference of State Legislatures. "State Security Breach Notification Laws." Web. <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>. Last updated, August 20, 2012.

[31] National Consumer Law Center. "Consumer Protection in the States: A 50-State Report on Unfair and Deceptive Acts and Practices Statutes." Rep. Boston, Feb. 2009. Web. <http://www.nclc.org/images/pdf/udap/report_50_states.pdf>.

ISA Response:
As stated in the ISA co-authored trade association white paper, "Improving Our Nation's Cybersecurity through the Public-Private Partnership":

> "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."

In sum, it is recommended that "Government and industry [] utilize existing standards and work through consensus bodies to develop and strengthen international standards for cybersecurity."

Use of Frameworks, Standards, Guidelines, and Best Practices:
As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

"Use of Frameworks, Standards, Guidelines, and Best Practices" Section Questions and ISA Responses:

1. What additional approaches already exist?

ISA Response:

Each year, Verizon and Secret Service undertake an analysis of actual data breaches that occurred during the previous calendar year. According to their 2012 Report, 97% of breaches were avoidable through the usage of simple or intermediate controls.[32] The report, as it has done in previous years, then provided a list of those controls.[33]

Jim Lewis of the Center for Strategic & International Studies found similarly, stating in his February 2013 paper that survey data has shown that 80 to 90 percent of successful breaches of corporate networks required only the most basic techniques and that if the top measures suggested by both the United States' National Security Agency and the Australian Defense Signal Directorate were used, then corporations could see their risk of breach fall "by 85 percent" and "in some cases, to zero."[34]

The ISA has also examined how best to utilize scarce resources and mitigate against cyber threats. Based on a series of conversations and jointly held corporate workshops with the American National Standards Institute (ANSI), ISA and ANSI soon discovered that traditional approaches to cyber defense such as perimeter defense were largely reactive and were failing to keep pace with the evolving nature of the cyber threat. Rather, what sophisticated corporations were advocating for and finding success with was an enterprise-wide, risk management strategy.

In 2008, ISA and ANSI released their first publication, "The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask," which described this approach and provided a series of questions that cross-departmental authorities such as CEOs or CFOs should ask its departmental heads. In 2010, ISA and ANSI released their second publication in the series, "The Financial Management of Cyber Risk: An Implementation Framework for CFOs," in which they laid out a series of measures that a corporation should take to implement this risk management approach.

Those measures are described below:

---

[32] 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>.

[33] Verizon. "2012 Data Breach Investigations Report." Rep. March 22, 2012, pp.61-66. Web. <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf>.

[34] Lewis, James A. "Raising the Bar for Cybersecurity." Center for Strategic & International Studies. Feb. 12, 2013, p.1.

Eliminate unnecessary data and keep tabs on what's left (Verizon 2011, Executive Summary, p.4).

Ensure essential controls are met and regularly audit to in order consistent implementation: "Identifying a set of essential controls and ensuring their implementation across the organization without exception, and then moving on to more advanced controls where needed is a superior strategy against real-world attacks." (Verizon 2009, C&R, p.44).

"**Change default credentials:** Simple and sweet, when system/network admins stand up a new system, change the password. If you outsource this to a third party, check that they've changed the password. Don't assume that your staff or your partners consistently follow through on all policies and procedures…" (Verizon 2011, C&R, p.65).

"Avoid shared credentials: Another obvious yet frequently omitted and oft-exploited problem. Along with changing default credentials, organizations should ensure that passwords are unique and not shared among users or used on different systems. The use of shared credentials allowed quite a few breaches …. This was especially problematic for assets managed by a third party." (Verizon 2009, C&R, p.46).

Implement a firewall or access control list (ACL) on remote access/administration services: "In many instances, remote access services have been enabled and are Internet-facing. We recommend tying these services down where only specific IP addresses or networks can access them. Additionally, it's important to limit access to sensitive systems within the network. Many organizations will allow any device on the network to connect and remotely access any other device; we highly recommend not managing your devices this way. Tie down remote access services to specific management networks via access control lists." (Verizon 2011, C&R, p.66).

Utilize IP Blacklisting: "consider blocking large address blocks/regions if they have no legitimate business purpose." (Verizon 2012, C&R, p.63).

Update anti-virus and other software consistently: "For every vulnerability exploited by hacking and malware attacks in 2008, the patch necessary to prevent the breach had been available for at least six months prior to the incident. In fact, all but one had been around for a year or more. While it may seem logical to conclude that organizations aren't patching fast enough, this is not the correct interpretation. All of these organizations had patch cycles well below the six month mark. The problem throughout all five years of this study has far more to do with scope than speed. Organizations would find much more value if they divert resources from patching ever-faster to patching more consistently and comprehensively." (Verizon 2009, C&R, pp.46-47).

Audit User Accounts: "Prior year's data breach reports and years of experience lead us to believe in the value of reviewing user accounts on a regular basis. The review should consist of a formal process to confirm that active accounts are valid, necessary, properly configured, and given appropriate (preferably least) privileges." (Verizon 2011, C&R, p.66).

"Restrict and monitor privileged users: Trust but verify. Use pre-employment screening to eliminate the problem before it starts. Don't give users more privileges than they need (this is a biggie) and use separation of duties. Make sure they have direction (they know policies and expectations) and supervision (to make sure they adhere to them). Privileged use should be logged and generate messages to management. Unplanned privileged use should generate alarms and be investigated." (Verizon 2011, C&R, p.66).

Monitor and filter outbound network traffic: "At some point during the sequence of events in many breaches, something (data, communications, connections) goes out that, if prevented, could break the chain and stop the breach. By monitoring, understanding, and controlling outbound traffic, an organization will greatly increase its chances of mitigating malicious activity." (Verizon 2011, C&R, p.66).

"Application testing and code review: SQL injection attacks, cross-site scripting, authentication bypass, and exploitation of session variables contributed to nearly half of breaches attributed to hacking or network intrusion. It is no secret that attackers are moving up the stack and targeting the application layer. Why don't our defenses follow suit? As with everything else, put out the fires first: even lightweight web application scanning and testing would have found most of the problems that led to major breaches in the past year. Next, include regular reviews of architecture, privileges, and source code. Incorporating a Security Development Life-Cycle (SDLC) approach for application development is recommended as well. Finally, help your developers learn to appreciate and write more secure code." (Verizon 2011, C&R, p.66).

Monitor and mine event logs: "All too often, evidence of events leading to breaches was available to the victim but this information was neither noticed nor acted upon. Processes that provide sensible, efficient, and effective monitoring and response are critical to protecting data. However, don't just focus your logging efforts on network, operating system, IDS, and firewall logs and neglect remote access services, web applications, databases, and other critical applications. These can be a rich data set for detecting, preventing, and investigating breaches." (Verizon 2011, C&R, p.66).

"Change your approach to event monitoring and log analysis: Based on the data we collect in the Time of Breach events, we believe that organizations would be better served to focus less on the "real-time" methods of detection, and more on the "this-week" methods. If we can shift Compromise to Discovery time frame from Weeks and Months to Days, it will significantly reduce the damage done to your organization. Focus on the obvious things rather than the minutia. This need not be expensive; a simple script to count log lines/length and send an alert if out of tolerance can be quite effective. We are confident that this approach will reap benefits and save time, effort, and money." (Verizon 2011, C&R, p.67).

"Define 'suspicious' and 'anomalous' (then look for whatever 'it' is): This is admittedly vague, but—in truth— generalizing what this entails in order to prescribe something for everyone would counteract the point. Discover what is critical, identify what constitutes normal behavior, and then set focused mechanisms in place to look for and alert upon deviations from normality." (Verizon 2011, C&R, p.66).

"Increase awareness of social engineering: Educate employees about different methods of social engineering and the vectors from which these attacks could come. In many of our cases, we see where users click on links they shouldn't and open attachments received from unidentified persons. Reward users for reporting suspicious e-mail and sites and create the incentives necessary for vigilance." (Verizon 2011, C&R, p.67).

"Train employees and customers to look for signs tampering and fraud: Such awareness campaigns have been around in certain areas for some time, but ATM and Pay-at-the-Pump tampering/fraud seem to be increasing in number and scope. Organizations operating such devices should consider conducting regular examinations of them. Additionally, empower customers to help protect themselves as well as aiding the organization in spotting potential issues." (Verizon 2011, C&R, p.67).

"Create an Incident Response Plan: If and when a breach is suspected to have occurred, the victim organization must be ready to respond. An effective Incident Response Plan helps reduce the scale of a breach and ensures that evidence is collected in the proper manner." (Verizon 2011, C&R, p.67).

"Engage in mock incident testing: I mean listen, we're sitting here talking about practice; not an incident, not an incident, not an incident—but we're talking about practice (sports fans among you might get that reference). Yes, we are talking about practice, because practice makes perfect. In order to operate efficiently, organizations should undergo routine IR training that covers response strategies, threat identification, threat classification, process definition, proper evidence handling, and mock scenarios." (Verizon 2011, C&R, p.67).

"Secure business partner connections: Basic partner-facing security measures as well as security assessments, contractual agreements, and improved management of shared assets are all viewed as beneficial in managing partner-related risk." (Verizon 2009, C&R, p.44).

The Top 5 Combined Security Measures Suggested by the National Security Agency, the Australian Defense Signal Directorate, and CSIS's Jim Lewis That Have Proven Effective in Thwarting Attacks

Use application "whitelisting": "Use application "whitelisting" to help prevent malicious software and other unapproved programs from running – DSD regards this as the most important step companies can take. Rather than trying to identify and block malicious software, which creates the possibility that previously unknown attacks will not be stopped, using a "whitelist" means that only approved programs can run on a machine. This step eliminates much of the risk from malware." (Jim Lewis, pp.7-8).

Patch software: "Patch applications such as PDF readers, Microsoft Office, Java, Flash Player, and web browsers. These applications are in daily use in most companies. Patching closes off avenues that hackers will otherwise exploit. Software companies send patches to rectify or eliminate exploitable flaws or weaknesses in a system's design or operation found after it was sold (similar to a recall notice for an automobile). Often, patches are developed in response to the discovery of a successful hack. A failure to install the patches leaves systems vulnerable. Most companies already have some kind of patching system in place, but research suggests that

even with these systems, 5 to 10 percent of computers will 'miss' a patch. This means that mitigation works if it is paired with automatic monitoring." (Jim Lewis, p.8).

Patch operating systems: "Patch operating system vulnerabilities, for the same reasons discussed above. All operating systems have potential vulnerabilities; when software companies find and offer a fix, not using that fix leaves the users susceptible to criminals and foreign intelligence agencies, who expend considerable effort to find these 'holes' and exploit them." (Jim Lewis, p.8).

Minimize the number of users' administrative privileges: "Minimize the number of users with administrative privileges, the highest level of authority to make changes or undertake actions on a network. Easy access to administrative privileges let criminals who obtain them (and this is a frequent initial goal for most hackers) to install malicious software and change settings to make it easier to exfiltrate data and to hide their criminal activities." (Jim Lewis, p.8).

Continuous monitoring for risk: "Continuous monitoring does not mean a round-the-clock watch of a computer screen by a human being. This approach uses the built-in ability of computers to monitor and log performance. Some continuous monitoring systems generate data by comparing network performance and configuration to specific standards and known vulnerabilities…Continuous monitoring allows companies to observe the behavior of their networks and take rapid action to stop problems and is a critical complement to mitigation…It allows companies to automatically collect data on the behavior of their networks and generate quantifiable data that allows them to identify risks. It lets them verify that their security measures are working…." (Jim Lewis, p.10).

ISA Suggested Security Measures to Enable an Effective Risk Management Approach to Combating Cyber Attacks

Executive with cross-departmental authority to hold strategic control of cyber systems: "By now virtually every organization has integrated the wonders of the digital revolution into their business plan with respect to record keeping, supply chain management, online sales, and more. The unfortunate downside of digitalization – data security – has largely been relegated to an isolated, and often under-funded, operational department. Senior executives with cross-departmental authority such as CEOs or CFOs (or CROs) must take strategic control, not operational control, of the cyber system that is the nerve center of their corporate operation. These executives must appreciate, or learn, if need be, the true role that technology plays in the modern organization, including the financial risks that technology places on the organization and the steps that must be taken to manage risk appropriately." (ISA-ANSI, Financial Management of Cyber Risk, Step 1, p.14).

Appoint a Cyber Risk Team: "It is unrealistic to expect that senior executives would be able to determine all of the questions, let alone all of the answers, to the multiplicity of cyber issues that are generated within their organizations' various departments. Yet the financial importance of cybersecurity and its many ramifications means that senior executives cannot afford to delegate the subject entirely to specialists or to junior managers. This means that executives should take the step of forming and leading a Cyber Risk Team that can address cybersecurity from a strategic perspective. This team will need to obtain input from the affected stakeholders

and relevant professionals, assess this input and feedback, and make key strategic decisions from an enterprise-wide perspective…" (ISA-ANSI, Financial Management of Cyber Risk, Step 2, p.15).

Meet Regularly: "A face-to-face setting is ideal for the initial meeting of the Cyber Risk Team. Where an in-person meeting may be difficult in some geographically disparate organizations, at minimum an initial teleconference or videoconference should be held. Subsequent regularly scheduled follow-ups should occur, ideally in the form of quarterly check-ups. The regularity of these meetings is important since cyber threats and attacks, as well as mitigation strategies, shift frequently. Face-to-face discussions can be particularly useful to counter the challenges of separate business units that don't "speak the same language." Meeting in person is important because approaching what will be a novel issue in a potentially novel fashion may well lead to misunderstandings, both with respect to organizational strategy and the unique perspectives of various departments." (ISA-ANSI, Financial Management of Cyber Risk, Step 3, p.15).

Develop and adopt a cyber risk management plan across all departments: "The Cyber Risk Team should determine which actions and roles, either existing or new, are to be allocated to each functional area and establish the means through which to communicate and coordinate among the functional areas. The result should be a well-defined, holistic information security architecture. The plan needs to include provisions for increasing employee awareness as to the criticality of cyber systems and data. Employees must be clear about company policies on data categorization, data retention, and incident response. The enterprise's plan also needs to include provisions for securing connections with business partners, out-sourced suppliers, and other remote connections. The plan should also include a formally documented incident response and crisis communications plan to notify stakeholders (and the media, when appropriate), since even the best-protected companies cannot eliminate the real risk of a cyber incident that results in a "crisis" to be managed. In the wake of a cybersecurity event, an effective communications strategy can materially minimize the potential financial harm – including the "indirect" costs of potential damage to a company's reputation, its brand, its customer loyalty, and its employee's morale. All of these factors can have substantial impact on shareholder value." (ISA-ANSI, Financial Management of Cyber Risk, Step 4, pp.15-16).

Develop and adopt a total cyber risk budget: "Based on the Cyber Risk Plan, the cross-organizational team should calculate the gross financial risk for the organization. [I]t is important for senior management to understand the potential financial impact of a cybersecurity event, which can be substantial…Whichever [risk] formula an organization chooses, it is important to run this calculation through a cross-departmental risk management team to get a true enterprise-wide perspective on financial cyber risks and to develop a consensus on the budget." (ISA-ANSI, Financial Management of Cyber Risk, Step 5, p.16-18).

Implement, Analyze, Test, and Feedback: "The Verizon forensic analysis of 500 actual enterprise security breaches (cited earlier) found that in nearly 60% of the incidents, the organization had policies in place that may well have prevented the breach, but failed to follow them.[35] As detailed in the later chapters of this publication, it is important that the cyber risk management plan developed use clear metrics and that these metrics, including audits and penetration testing, be reviewed regularly both in terms of cyber risk management and budget.

[35] Verizon. "2008 Data Breach Investigations Report." Rep.

The results of these examinations and tests should be used as feedback to update and upgrade each segment of the cyber risk management plan. According to the Verizon study, in 82% of the cases examined, information about an upcoming attack was already available and either went unnoticed or was not acted upon. It is also important to focus on security basics rather than becoming focused solely upon sophisticated attacks. Verizon found that in 83% of the attacks studied, breaches came from attacks not considered to be very difficult to handle. In these cases many organizations were apparently so focused on stopping sophisticated attacks they failed to take care of the basics. Cybersecurity is an ever-evolving field. Even with broad application of the program and suggestions herein, strong financial incentives still favor the attackers. Thus, organizations can expect new threats to emerge in an attempt to circumvent the defensive measures that they have put in place. Organizations will need to continuously monitor and improve upon their cybersecurity policies over time to maximize their security and, ultimately, their profitability."

2. Which of these approaches apply across sectors?

ISA Response:
The above mentioned controls apply to all sectors.

3. Which organizations use these approaches?

ISA Response:
Much of the ISA membership uses these controls.

4. What, if any, are the limitations of using such approaches?

ISA Response:
As stated throughout this document, the major obstacle in implementing the above security measures (or any security measure) is cost. In 2009, President Obama commissioned staff from the National Security Council to conduct an intensive review of our nation's cyber security entitled the "Cyberspace Policy Review" (CSPR), which found that "many technical and network management solutions that would greatly enhance security already exist in the marketplace but are not always used because of cost and complexity."

The CSPR's finding has been confirmed by multiple independent studies from PricewaterhouseCoopers, McAfee and CSIS, CIO Magazine and the Ponemon Institute, which have been referenced repeatedly throughout this document and which have shown that despite nearly a near doubling of private sector investment in cyber security in the past 5 years "cost" remains the single biggest barrier to further improvements in cyber security.

Attempting to address critical infrastructure cyber security without directly addressing the single biggest obstacle - costs - is an unsustainable policy position. Accordingly, in order to encourage corporations to adopt and implement these controls, the U.S. Government should provide incentives for doing so. This subject of incentives is more fully discussed in the ISA Response to Question 5 below.

5. What, if any, modifications could make these approaches more useful?

ISA Response:
Because cost is the number one barrier to cyber security control adoption, as discussed above, the Government can encourage the adoption of the above described controls through the establishment of an incentive system. The Executive Order's Section 8(d) requirement that the Secretary of the U.S. Department of Homeland Security coordinate the establishment of a set of incentives following the issuance of incentives analysis reports from the U.S. Departments of Commerce, Homeland Security, and Treasury is entirely appropriate and necessary to help overcome this cost issue.

In order to establish an effective incentive system, however, there needs to be two essential elements: First, there must be agreement on which standards or practices qualify an organization for the economic benefit – such as an agreement concerning the qualification of the security controls discusses in the ISA response to this section's Question 1. Second, a system of incentives powerful enough to motivate adequate corporate investment must be tied to the standards, practices and processes that will generate enhanced security.

6. How do these approaches take into account sector-specific needs?

ISA Response:
The set of controls discussed in the ISA Response to Question 1 of this section apply across sectors and have been shown to be highly effective in combating an overwhelming majority of cyber attacks. See the ISA response to Question 1 for further discussion.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

ISA Response:
As discussed above in the ISA Response to Question 12 in the "Current Risk Management Practices" Section, there are already many sets of standards and best practices designed for security purposes. Some of the standards and practices are developed by government entities such as NIST, some by standards setting organizations such as ISO or ANSI and still others by entities, such as the ones described above in ISA Response to Question 1 above. One reason for the multitude of standards and practices is that there are multiple different systems and configurations of systems and these systems exist for varying purposes operating in various cultures. No one size of standards or practices "fits all."

While Sector Specific Agencies (SSAs) (and the U.S. Government) can certainly help in developing standards, it should be as a participant in the consensus-based standards setting process. The key issue for SSAs (and the U.S. Government at large), however, ought not to be who or where the standards and practices are developed, but how well they work. If certain sets of standards, measures, etc., are judged to be effective like the ones described in ISA Response to Question 1, then the SSAs should work with the private sector in developing a menu of market incentives to encourage the private sector to adopt these standards. This incentive-based approach is discussed more fully in ISA Response to Question 5 above and Question 8 below.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

ISA Response:
Security is not a binary issue; systems are not entirely secure or insecure. Correspondingly, security controls for these systems often have different levels of effectiveness. Accordingly, security control effectiveness can be measured on a sliding scale. For example, with respect to pharmaceuticals, over-the-counter pain relievers are effective to a certain extent with comparatively low risk associated. Prescription drugs maybe even more effective, though they carry higher risks, while hospital-only/M.D. directly supervised drugs can be most effective as well as most risky. Thus, with pharmaceuticals, it is public policy to allow drugs with a determined level of effectiveness compared to its risk to receive a wider access to market than those with higher risks.

A similar sliding scale could also apply in cyber security and with respect to the security controls described in the ISA response to Question 1 of this section. In sum, this 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.

Once the federal government, most likely through DHS, determines the effectiveness level of a particular method, sector specific agencies, operating under authority and oversight from their jurisdictional Congressional Committees, can then determine what incentives in collaboration with the sector coordinating councils ought to be applied to the varying levels of security.

Specific Industry Practices:
In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

"Specific Industry Practices" Section Questions and ISA Responses:

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

ISA Response:
See ISA's response to Questions 5 and 6 in the "Current Risk Management Practices" Section.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

ISA Response:
As mentioned, ISA's membership consists of some of the most cyber sophisticated companies. Many of these companies do have formal escalation processes for cyber security risks that either suddenly increase in severity or velocity. For example, there a number of ISA companies that have established security operations/intelligence centers that are not only tasked with monitoring cyber security risks, but also gaining intelligence, and responding/mitigating these risks if they become more immediate or realized. At a certain defined point in the attack life cycle, each organization's attack responders call in appropriate department officials (e.g., heads of Legal, Operations, PR, etc.) as well as the higher-ranking "business players."

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

ISA Response:
As described above, there are already adequate best practices and standards being developed to provide substantial safeguards to information systems. The U.S. government, via various entities (including NIST), already plays an active role in their development and should maintain that participation.

However, with possible specialized exceptions for unique systems, the U.S. ought not to seek to develop their own standards for use by "American" companies. In an inherently international economy, a set of "U.S. standards" could create a counterproductive international response and international "standards-race."

Rather, the US government ought to devote its resources to funding the analysis and evaluation of the already-developed, consensus standards that are market-available and provide incentives for enterprises to implement the standards that are determined to be effective. Remember, cyber networks and infrastructure constitute a global system where traditional borders do not apply. Not only are our companies and networks global, but so are our adversaries'. This global attribute must be taken into consideration for any policy or operational aspect of cybersecurity. The companies that fuel our nation's economic growth are operating globally in one way or another. They either have business operations in many other countries, source their products and services globally, or rely on just-in-time delivery of components or products to meet their domestic customers' needs. Therefore, we cannot deliberate public policy with merely a segmented, national lens.

Indeed, a "U.S." Framework will only heighten skepticism by global customers regarding the U.S. government's access to their corporate or consumer data and the implications of that access. Customers will simply go elsewhere to find providers that do not pose the same concern. Moreover, such a Framework will surely impact American companies' global competitiveness, interoperability, and would most likely result in copycat policies in other countries.

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

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

ISA Response:

ISA maintains that a system of mandated standards would be counterproductive and will not help protect against the types of attacks described in the Executive Order, namely cyber attacks that would result in a regional or national catastrophe. The types of attacks that would cause this damage would not be your "garden variety" DDoS attacks, perpetrated by the stereotypical kids in the basement. Rather, such attacks would be "designer" in nature, evading published Framework "practices," and would be formulated highly sophisticated, well organized, well funded, often state-sponsored attackers. In short, these attacks, at times referred to as the Advanced Persistent Threat, are perpetrated by the "pros"; if these attacks and attackers target a business or IT system, they will most likely succeed in at least penetrating or "breaching" such a system.

This does not mean that there are no defenses, however. Indeed, many companies have been working for several years with some success on mitigating APT attacks. To combat these types of attacks, companies have moved from more of a perimeter defense strategy concerned with stopping breaches to allocating resources toward internal system monitoring and threat detection with subsequent mitigation. Traditional approaches, including compliance with a set of required "practices" will not solve the problem as such an approach would be largely reactive and would not stay ahead of the changing nature of the threat. Worse, such requirements could be counter-productive, leading companies to expend their limited resources on building in-house efforts to meet these new regulatory demands rather than dealing with the threat proactively. Accordingly, any framework should be light on specific, prescriptive practice requirements and should examine already available, consensus-based, dynamic security controls that have been proven effective and tie incentives to their voluntary and repeat adoption.