Booz | Allen | Hamilton

13200 Woodland Park Road
Herndon, VA 20171

April 29, 2013

Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
Attn: Alfred Lee
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230
cyberincentives@ntia.doc.gov

Re: Notice of Inquiry – Incentives to Adopt Improved Cybersecurity Practices (Docket Number 130206115-3115-01)

Dear Mr. Lee:

Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," seeks to enhance the cybersecurity of the Nation's critical infrastructure through among other things, improved information sharing, joint government and industry development of a framework of cybersecurity practices to reduce risk, and voluntary adoption of that framework by critical infrastructure owners and operators. Furthermore, EO 13636 directs the Secretaries of Commerce, Homeland Security, and Treasury to provide the President separate analyses and recommendations on how best to incentivize adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework and participation in the Department of Homeland Security's voluntary Cybersecurity Program. While analyzing and making recommendations on incentives is a necessary step, successful adoption of the Cybersecurity Framework is dependent on government and industry putting incentives in place that are powerful enough to influence corporate behavior and match the level of investment necessary to implement future cybersecurity practices and standards.

Booz Allen Hamilton (Booz Allen) has a long history of working cybersecurity-related challenges across the public and private sectors, including information assurance, cybersecurity operations, cyber threat intelligence, data analytics, advanced malware detection, and communications security. We operate throughout the entire lifecycle of cybersecurity, partnering with clients in diagnostic and strategy-setting, designing targeted capability solutions, and finally, implementing and operating those solutions. Both government and industry face the challenge of defining and implementing cybersecurity practices to address the evolving threat landscape. There are a variety of incentives, which can change behaviors; however, they must be put into the context of the business

environment and address the challenges associated with adoption of cybersecurity solutions.

THE REALITIES OF CYBERSECURITY INVESTMENT

Regardless of an organization's size, cybersecurity investments are often evaluated as a function of an organization's total information technology (IT) budget. As one example, in the financial services industry, Booz Allen Hamilton (Booz Allen) has seen that top U.S. firms spend around four percent of their annual operating budget on cybersecurity. However, this number varies greatly by company, and is dictated not only by budget, but also by whether security is embedded in a company's lines of business or is a back office support function. Some view the costs associated with IT and cybersecurity in the financial services industry as a support function rather than a revenue generating capability. In today's economic environment, there are incentives to keep security costs as low as possible.

Additionally, organizations face other challenges in investing in and applying cyber protective measure to one's enterprise.

- First, some managers see the perceived need to adopt, incorporate, and maintain cybersecurity solutions as too burdensome—in terms of both time and treasure. For example, some industries could regard the majority of cyber intrusions as largely nuisances, small dollar incidents where the organization can easily absorb the costs of preventative measures and response actions by passing the costs on to customers via higher fees or prices. Only when these smaller events grow to a significant number and dramatically impact the bottom line will companies begin to invest in more significant protective measures.

- Second, it can be difficult for an organization to assess the benefits of protecting a network: how does an organization quantify a return on security investment for a network intrusion that never happened because a firewall or intrusion detection system prevented it from occurring? Organizations weigh a potential investment in terms of return on investment, which is challenging to do in the context of preventing a cyber incident. Paradoxically, the more effective the security measures, the higher the likelihood that the organization will reduce future funding as the aggregate number of intrusions and attacks appears to shrink.

- Third, the cost of IT protection is often concentrated within an organization (e.g., Chief Information Officer or Chief Information Security Officer), while the benefits of protecting networks are highly distributed. In other words, the entire organization benefits from good cybersecurity, but the bulk of the spending occurs in one cost center (and is often considered overhead), making cyber spending vulnerable to reductions.

- Fourth, the revelation of a cyber intrusion is not something a commercial enterprise wants. There is a counter incentive, albeit a strong business incentive, for companies to refrain from sharing information about an attack out of a concern that publicity about such an event can cause bad public relations and/or create a negative impact on shareholder value.[1]

Many companies make business and financial calculations regarding cybersecurity in a vacuum as they lack a standardized methodology and process to effectively evaluate investments. We believe that companies should include the "hard costs" (the costs of protective hardware and software) and "soft costs" (financial impact to brand, reputation, and shareholder value) into a specific, organizational-centric investment management system. This system would align strategy, resource allocation, and performance management allowing for greater, efficient capital allocation throughout the entire cybersecurity planning process.

CREATING INCENTIVES FOR CYBERSECURITY

An incentive is defined as "something that incites or has a tendency to incite a determination or action."[2] Before organizations can identify effective incentives, and more importantly implement them, government and industry must work together to define the desired "actions" (i.e., behaviors) in cybersecurity that critical infrastructure organizations need to invest in.

Through our experience in supporting government, commercial, and international clients, we have found that cybersecurity practices must be efficient and effective in dealing with current and future threats and vulnerabilities, cultural shifts, business needs, and technological advancements. At the same time, they must enhance the overall preparedness and resilience of critical infrastructure and reduce risk to a sector (and the nation). A one-size-fits-all "checklist" of cybersecurity controls runs counter to this idea and is limiting, as different sectors have different priorities and risk profiles vary across sectors. For example, the Electricity Sub-sector is highly concerned with the resilient operation of its control systems environment as compared to the Financial Services Sector, which is more concerned about information leakage and denial of service through the information technology environment. While the Healthcare Sector shares concerns about information leakage with its financial services colleagues, much of the sector's time, energy, and resources are tied to reforming healthcare payment and delivery operations and implementing electronic health record meaningful use regulations. Organizational priorities and risk profiles also vary depending on the size of the institution and its global reach. A Framework that adjusts to and accommodates the unique operating and risk environments of various business types—while still maintaining an overall common foundation—holds the potential for enhancing cybersecurity at the sector- and national-level and for designing and implementing incentives that help provide a means to that important end.

---

[1] Sulek, David and Doscher, Megan. "Beyond Public-Private Partnerships: Leadership Strategies for Securing Cyberspace" *Cybersecurity: Public Sector Threats and Responses.* Ed. Kim J. Andreasson. CRC Press, 2011. Print.
[2] Merriam-Webster Dictionary

The Federal Government should use existing government centers of excellence and industry "utilities" (e.g., private sector Information Sharing and Analysis Centers, industry research institutes, etc.) to develop a consistent set of cybersecurity standards, platforms, or policies from which to build. This should also incorporate proposals made by leaders in private industry around computer hygiene—a set of basic practices, standards, and policies that represent a minimum level of cybersecurity and that will increase adoption in those enterprises and sectors lagging behind early adopters. We have found that an approach grounded in a risk-based philosophy of measuring, managing, and maturing functional (e.g., threat intelligence, application security, infrastructure and mobile security, etc.) and enabling (e.g., governance, policies, awareness and training, change management, etc.) controls can be applied efficiently and effectively with multiple sectors, increase the overall security posture of an organization, and provide a foundation for consensus-driven standards. Specifically, these types of standards can help ensure that usability/convenience increases while costs decrease (or that costs are more easily justified) over time.

Given the realities of business operations, what it takes to "incite" an organization (or a Sector) to take action will vary from business to business within a Sector and among Sectors. To be effective, incentives need to be oriented toward the **business drivers** that matter most to the senior management of private sector critical infrastructure organizations—the bottom line/shareholder value; brand and reputation; and risk management. Incentives can use rewards and penalties to drive action, performance, and results. A menu of incentives should be provided by government and industry to incite action, particularly among late adopters and skeptics.

Table 1: Menu of Incentives for Cybersecurity and Critical Infrastructure Resilience

Business Driver	Incentives
Maintain or Raise Shareholder Value	- Tax Breaks for Investments in Cybersecurity Solutions - Grants or Subsidies for Cybersecurity Solutions and Innovation - Regulatory Consistency and Relief - Baseline Economic Measures that visibly justify cyber expenditures in terms of absolute costs and return on investment
Protect Brand and Reputation	- Liability Protection for Information Sharing - Certification/Recognition/Award for Cyber Excellence
Manage Risk to the Bottom Line	- Cyber Liability Insurance - Regulation and Compliance (e.g., Sarbannes-Oxley) - Shared Sector Services (e.g., threat intelligence, authentication, etc.)

THE CHALLENGE OF ADOPTION

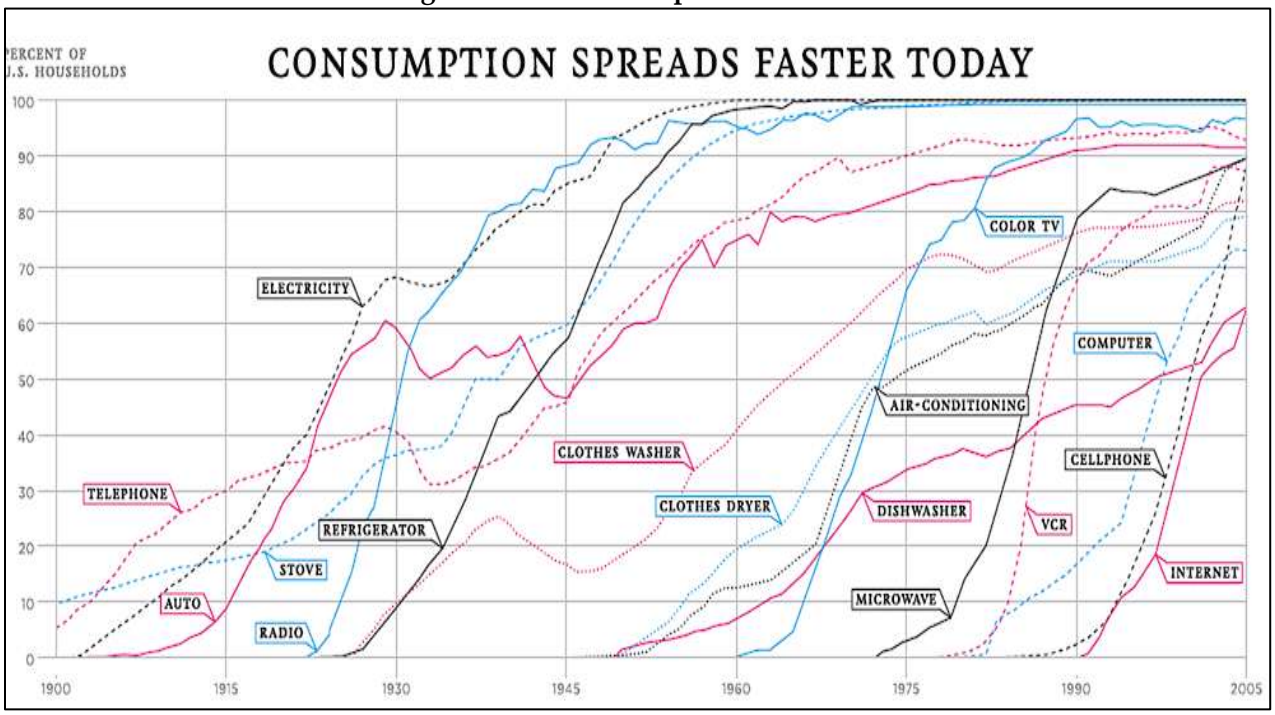
For every major technology revolution of the past century (e.g., electrification, the television, the personal computer, Internet access, online sales, etc.) the story of adoption has followed a similar path. New products, which are revolutionary are introduced—but pundits claim companies will never use them; once acquired, they will be too expensive to install, hard to use, and difficult to justify the return on investment; and even when implemented successfully, corporate users and customers will struggle to adjust to the system and workflow changes. Yet, in far fewer years than expected, these types of

products become ubiquitous and indispensable. By exploring when, how and why certain products or solutions succeed in winning substantial market share and adoption, we can better understand the factors that: (1) have traditionally inhibited the widespread adoption of cybersecurity solutions and (2) point to some possible strategies to stimulate greater adoption.

What Drives Adoption?

As first described by Everett Rogers in his 1962 book *Diffusion of Innovations,* successful technological adoption tends to follow an S-shaped growth curve. At first, products face difficulty in gaining traction (even among early adopters) because of their high cost and challenges implementing them within existing systems and workflows. Then, as early adopters demonstrate benefits and the products improve, convenience rises as costs decrease. Information about them is shared across personal and professional networks and adoption spikes. When this occurs, the product experiences exponential growth for a period. Eventually, it peaks and reaches the point of diminishing returns as it takes more and more time to reach the remaining smaller and smaller segments of the marketplace. Figure 1 illustrates some of the historic S-curves of the past century.

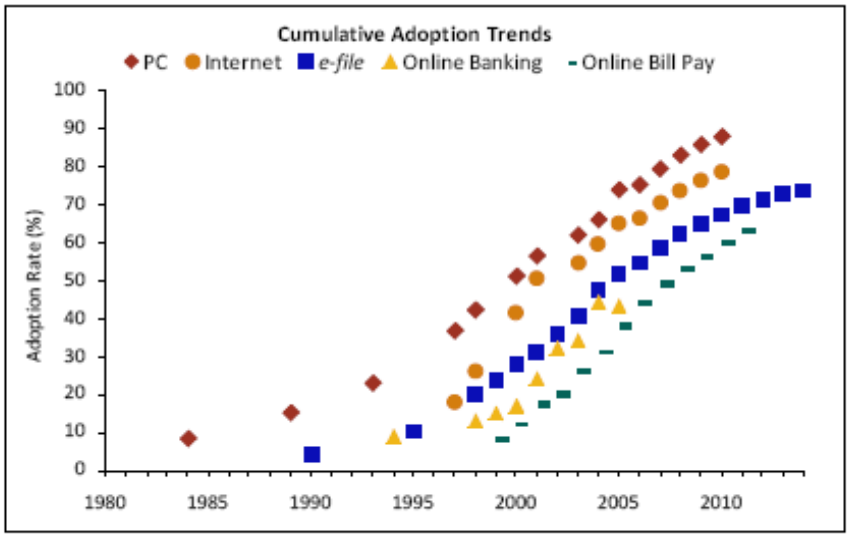
Figure 1: S-Curve Adoption Patterns[3]



In highly innovative periods, these patterns build upon one another in virtuous cycles. Figure 2 demonstrates how the personal computer and Internet access followed the traditional S-curve—and how the accompanying services that use that access followed suit (e.g., online banking, bill payment, travel reservations, and tax filing).

[3] W. Michael Cox and Richard Alm, "You Are What You Spend," *The New York Times*, February 10, 2008

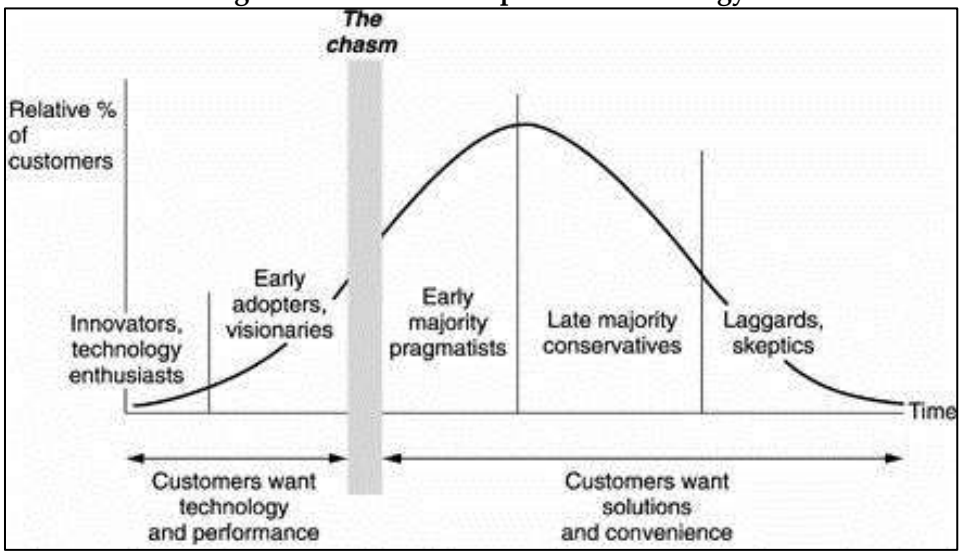
Figure 2: Cumulative Adoption Trends[4]



What explains the lack of cybersecurity adoption?

A key aspect of adoption is to understand the targeted customers. A common challenge in the adoption of a new product or solution is a "chasm" that forms between early adopters (10-15% of the target customer group) and the remaining customers.

Figure 3: Customer Adoption of Technology.



It is important to note that various types of cybersecurity products—such as public key encryption, intrusion detection systems, firewalls, and virtual private networks—have been around for more than 20-25 years and adoption rates a high. However, it took many years for these solutions to become ubiquitous and adoption rates continue to vary across economic sectors. Interestingly, companies have been slow to implement new cybersecurity solutions, particularly when compared to the rapid adoption of new enabling technologies

[4] The MITRE Corporation, "Advancing e-File Phase 1 Report," The Internal Revenue Service, 2008, p. 3

such as web-enabled solutions, social media, mobile computing and applications, and now cloud computing. *What explains this?* We believe there are three critical factors to explain why the adoption curve for cyber solutions and products is flatter than for other forms of technology innovation:

- **Sharing of Benefits:** as noted above, a critical aspect of accelerating and increasing adoption is the sharing of benefits across personal and professional networks. For products such as social media and mobile computing, the sharing of these benefits flows easily across enterprise and personal networks. The benefits are tangible and obvious: new enabling features, cost reductions, greater convenience. Three elements limit the sharing of cybersecurity benefits. The first is the limitations in professional and personal networks. While many economic sectors (e.g., financial services, energy, etc.) may share lessons within their sector, the sharing of this type of information across sectors is limited at best. For example, lessons learned by the banking industry around certain products or services may not be shared with others with similar needs, such as retailers or healthcare insurance payers; these individuals may not operate in common professional circles. The second is that the benefits of cybersecurity may not be as obvious or easy to share. The third is the sensitivities associated with cyber protections (why share a proprietary advantage if you have a gold-plated solution) or intrusions (would you reveal to a professional community a key corporate exposure).

- **Return on Investment:** a significant challenge surrounding adoption is quantifying the benefits of cybersecurity products. The issue centers on the concept of cost avoidance. To accurately assess the benefits of cybersecurity, a company needs to accurately assess the costs (hard and soft) avoided or mitigated through implementation. This can be difficult to calculate (how do you measure the impact of an attack that never happened?) and harder to justify. The lack of an economic baseline for the costs of various types of cyber attacks (e.g., denial of service, data breach, economic espionage) makes it extremely difficult to justify the expenditures on emerging cyber solutions.

- **Intermediaries:** while there are certainly standards published for cybersecurity by NIST and other bodies, a continuing challenge within the cyber industry is the development of highly specialized or proprietary solutions. In many ways, this is understandable. Developing advanced cyber solutions via open platforms exposes those solutions to would-be attackers. However, if one examines the adoption curve in other key technology areas, creation of common standards, platforms, or policies is paramount. For example, would the widespread adoption of washers, dryers, and refrigerators have occurred without Underwriter's Laboratories? Would electronic commerce have thrived without the emergence of intermediaries like VeriSign, PayPal, and others?

What could the U.S. Government and industry do to stimulate adoption?

We believe the following activities will close the chasm and accelerate or increase the adoption of cybersecurity solutions by private industry:

1. Continue to aggressively promote the concept of one or more information brokers, but with a greater dual emphasis on (1) stimulating cross-sector sharing and (2) expanding sharing beyond immediate threat information to include the benefits of cyber solutions. Accelerating nationwide adoption of cybersecurity technologies and solutions directly depends on the communication and sharing of the benefits of a strong cybersecurity program—what works, what benefits are accrued, in what timeframe, etc.—and continuous learning and improvement.

2. Develop an economic baseline for cybersecurity that will enable companies to assess the return on investment and convince those late adopters and skeptics to invest in cyber solutions. This economic baseline would need to account for differing types of cyber attacks and their bottom-line impacts and (potentially) industry variations in how risk is calculated, mitigated, and "bought down."

3. Establish independent, third-party organizations to govern the adoption of cybersecurity practices by Sectors. Sectors should define standards of practice (in coordination with regulators, where appropriate) against which the third-party organization is then responsible for assessing and evaluating the effectiveness of organizations to implement desired actions over time, thereby increasing their maturity and reducing overall risk to the Sector.

4. Promote cyber liability insurance to insure against loss of sensitive information in the digital realm. When an organization feels the need to obtain cyber insurance (due to a recent event or just being proactive), they engage an insurer who assesses the organization's risk profile. If not up to par, the insurer will require the organization to enhance security measures before a policy is offered and signed. The organization mitigates cyber risks in this process and enhances its security posture, and the insurer gains enhanced confidence in its ability to offer coverage. Cyber liability insurance represents both a financial incentive (i.e., protects an organization against loss, protects shareholder value) and a hidden penalty (i.e., over time insurance guidelines will establish higher standards of due care that will create costs for companies).

5. Establish a "cybersecurity excellence" awards program to stimulate the type of interest, innovation, and investment necessary for industry to rapidly adapt to the dynamic threat environment and enhance cybersecurity. For example, an approach could involve creating a "seal" program (e.g., The National Cybersecurity Excellence Seal) where industry applies to the program hoping to qualify for a Government seal or label. Government, industry, and civil society would create baseline standards collaboratively and individual companies would submit applications. Any number of applicants may qualify for an award and receive a seal of approval (as a general label or with qualifying levels (e.g., gold, silver, bronze)). Government could

evaluate applicants or companies could complete a self-assessment form. An annual event could be sponsored to dispense awards and facilitate the sharing of practices.

Thank you for the opportunity to provide Booz Allen's views on cybersecurity. We look forward to continuing the dialogue with the Department of Commerce and our partners in government and industry on this important topic.

Very truly yours,

John Michael "Mike" McConnell
Vice Chairman
Booz Allen Hamilton