Before the
DEPARTMENT OF COMMERCE
Internet Policy Task Force

	)	
	)	
In the Matter of	)	
	)	
Cybersecurity, Innovation	)	Docket No. 100721305-0305-01
	)	
and the Internet Economy	)	
	)	
	)	
	)	

COMMENTS OF TECHAMERICA

Liesyl I. Franz
Vice President, Information Security and Global Public Policy
TECHAMERICA
601 Pennsylvania Ave, NW
North Building, Suite 600
Washington, D.C. 20004
(202) 682-4434

September 20, 2010

TechAmerica hereby submits these comments to the Department of Commerce ("Department"). TechAmerica's members have a vested interest in the success and future of the Internet and TechAmerica is pleased to be able to file comments on their behalf in this proceeding.[1]

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation for the global innovation economy. Representing approximately 1,200 member companies of all sizes from the public and commercial sectors of the economy, TechAmerica is the industry's largest advocacy organization and is dedicated to helping members' top and bottom lines. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of the American Electronics Association (AeA), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics and Information Association (GEIA).

TechAmerica's members include: manufacturers and suppliers of broadband networks and equipment; consumer electronics companies; ICT hardware companies; software and application providers; systems integrators; Internet and e-commerce companies; Internet service providers; information technology government contractors; and information technology consulting and sourcing companies.

TechAmerica welcomes this opportunity to provide the Department's Internet Policy Task Force with a viewpoint shared by such a diverse membership.

[1] *Cybersecurity, Innovation and the Internet Economy*, Notice of Inquiry, 75 FED. REG. Number 144, Page 44216-44223 (July 28, 2010).

Introduction

TechAmerica believes strongly that the contribution of the technology industry to productivity, innovation and national economic growth is unparalleled. The proliferation of the Internet and the information economy has had a significant impact on every aspect of our society and the economy. The environment in which we face the challenge of cybersecurity is far more complex than just the Internet itself and includes the collection of IT and communications networks that are both huge and international in scope. However, with this growth and success, risks and weaknesses have also developed. This is why it is critical that the government and the private sector engage in a partnership to share information and minimize these risks. TechAmerica looks forward to continuing to work with the government to better secure our nation.

Quantifying the Economic Impact

The increased use and dependence on the Internet has led to an increase in the number of vulnerabilities to which we are exposed, both as individuals and as enterprises. As those vulnerabilities are exposed through system flaws or exploited by malicious actors, those compromises result in great financial loss, much of which is difficult to calculate. Through reports of system downtime, financial theft, incident response and mitigation efforts, and loss of intellectual property, various reports on economic impact of those costs have been promulgated. But, those calculations are incomplete estimates at best, and sorely understated at worst.[2] Based on aggregated analysis of existing reports, in 2008, 285 million consumer records were breached, and the financial repercussions of compromised online data rose to nearly $1 trillion.[3]

While a more accurate depiction of the actual and downstream financial loss from cybercrime/cyber attacks would be more useful, the information and thoughtful analysis we have today in these reports should not be discounted. It captures qualitative impact and helps illustrate the complexity of the challenges we are facing in cyberspace; as such, both government and industry have taken notice and taken action. With more in-depth analysis, individuals and organizations could take more efficient risk management or event prevention and mitigation efforts, and the pressure to demonstrate return on investment in the classic sense could be alleviated. Another approach is to study the costs required to achieve the current level of security. These costs are significant and are required to keep things just where they are today. With a better ecosystem, these direct costs should trend downwards.

All enterprises have one great incentive to protect themselves: to retain the trust and confidence of their customer in order to remain viable in the marketplace. Additional incentives that would help provide for enterprises to share information regarding their breaches (and, to some degree, the related financial loss), are: the existence of trusted foundries for information exchange between enterprises and, , between industry and government that provides for privacy protection, protection of

[2] Examples of such reports include, but are not limited to the annual Computer Security Institute’s survey, the Ponemon Institute's Cost of a Data Breach report, the RSA Online Fraud Report, the biannual Symantec Global Internet Threat Report, and the Verizon Business RISK Team Data Breach Investigations Report, among others.

[3] Aggregated analysis from example reports.

proprietary information, anonymity; a two-way value proposition that allows for all participants to benefit from the resulting analysis and trend studies. TechAmerica has long supported such a regime, and we continue to advocate for policies that enable and empower such a mechanism. The existing Information Sharing and Analysis Centers (ISACs) are one example of an infrastructure that could be bolstered for increased capacity and coordination and thus better data. Industry associations such as TechAmerica can also provide value as a coordinator and third party for its members and, as a result, to the greater stakeholder community. Given the scope of the problems we face and the diversity of the community, we should consider that not just one entity or framework provides the answer for all, and a synergy among various entities could also be helpful. No matter what mechanism(s) is used or created, it must accommodate the privacy of personally identifiable information, company proprietary information and copyright, and civil liberties concerns.

The loss of intellectual property and the downstream implications is very difficult to determine and as such is a data set that is missing from reports listed above. This is one area where more work needs to be done. In addition, many companies and groups are working to determine the opportunity costs associated with inadequate security. This analysis is easier to do today than it was just a few years ago, as we have more illustrative experience on which to draw conclusions, and risk management methodologies are more robust today as a result. However, for many companies, particularly small and medium-sized businesses, the cost is too great for the ultimate in preventative care. As such, TechAmerica recommends policymakers consider two opportunities to enable further action: (1) developing a refundable tax credit for security measures, including adoption of best practices as well as participation in the appropriate sector critical infrastructure protection efforts and ISACs; and (2) ensuring that security measures based on global standards are included in requirements for national programs (i.e. broadband and smart grid).

For any initiative that attempts to measure the economic impact, it should not focus solely on precise data and measurements but rather emphasize trending, patterns, and other broad ways of analyzing the information. In addition, economic analysis should include a comparison of civilian and military losses as well as a global analysis of the U.S. vis-à-vis other countries.

Raising Awareness

There are two elements of awareness that need to be addressed: informing and educating the individual user, and informing the community of enterprise users about the resources that are available to them for assistance in their cybersecurity efforts.

Regarding user education, there are many organizations, both public and private (corporations and not-for-profit organizations) that take on some level of effort regarding raising awareness for the end users. Each organization has their own mission and purpose, and each executes relevant programs to meet their targeted constituency. We are not aware of any analysis that has been done to categorize these efforts; that could be a useful endeavor if the goal is to find and leverage synergies in those disparate efforts.

More to the point, TechAmerica supports user education and awareness efforts, both in the classroom and out. We support a concerted, nationwide, public service campaign such as that as is being undertaken by the National Cyber Security Alliance (NCSA), which also sponsors staysafeonline.org. More funding and a focus on partnership could significantly bolster NCSA's good work to date. It is important to note that many companies engage in a variety of user awareness activities in their communities, in their cadre of employees, and in their customer base.

Regarding cybersecurity education programs, we do not have visibility into studies that analyze their effectiveness – at any level. However, we do have the sense that not enough training is occurring at the most obvious opportunity – the moment a child first logs on – or uses – a computer in school. A concerted effort at that stage would go a long way to building a culture of cybersecurity, cyber safety, and cyber ethics for the long term. Curricula should be developed that is appropriate for the target agegroup. In general, all awareness programs should be simple, basic, thorough to capture the fundamental best practices but be flexible enough to adapt as necessary.

At the older levels, we also have an opportunity to engage our students not only in ways they can protect themselves online but also to engage them in activities that can lead to their cultivation as the very engineers, programmers, and other technologists that will continue and enhance innovation in technology and security. While there is a smattering of creative training activities across the country, concerted training efforts such as cyber challenge competitions, apprentice programs, and internships can also be bolstered with greater senior level commitment and funding.

With regard to raising awareness in the industry about the resources available to them, the key phrase is: public-private-partnership. In both strategic risk management for critical infrastructure protection and in operational information sharing and analysis efforts, there is a robust program for engagement by virtually every enterprise in the country. Both the private and public sector partners in the National Infrastructure Protection Plan (NIPP) have an imperative to grow the partnership and to reach new participants. While many large enterprises, including notably those that engage in business with the government (either directly or as a sourced supplier), are familiar with the partnership under the NIPP, a great majority of small and medium-sized businesses across the country are not.   Even if they are aware of the program, their ability to participate may be low due to cost or to finding prioritized benefit and relevance. There may be ways to adjust the partnership structure to accommodate the specific needs of small and medium sized businesses. One way to address this gap is to utilize the bully pulpit more significantly than has been done to date. A clear and consistent message at the most senior level of government and industry about the opportunity and the value of participating in the partnership – both for the steady state and in a cyber emergency— will help with engagement. It is important that this endeavor not be seen as a government only – and government imposed – program, but rather one that is undertaken in partnership and coordination from the very beginning of the process. Otherwise, the fear of government intervention will deter industry participation. Government and industry can partner through the NIPP Coordinating Councils, the ISACs, and, industry associations that can reach across the country to their members and customer base.

With regard to resources, more can be done to inform the government and business community about ways they can get more information about technology trends, risk management and mitigation efforts, technical assistance, partnership opportunities, and other benefits. It is important to note, however, that some of these services exist in the marketplace today, and direct duplication would hamper competition and competitiveness and in the worst case, diminish security. For example, when considering technical assistance options, the government may or may not be in the best position to provide service to a set or subset of industry stakeholders. In those instances, dialogue and partnership is the key.

Finally, an invaluable component of raising awareness for enterprise users is the ability to provide them information about current and evolving threats. . We have long been challenged by the inability to share useful and actionable threat information between industry and government, but we need to find a way to do it.

Web Site and Component Security

The NOI poses the question whether the government alone, the private sector, or the government and the private sector collaboratively explore whether third-party verification of web site and component security is, or can prove effective in reducing the proliferation of malware. The question as posed does not accurately reflect the problem. The majority of malware online is not due to insecure websites themselves. Malware online and the security of websites are two distinct issue that should be dealt with separately. TechAmerica posits that this kind of analysis – and innovation – is already underway in the private sector and may not need government intervention. If government is involved, it should be in partnership in order to address cost, collaboration, and cooperation in the environment. Additional questions would include what standards to use, depending on risk; how to identify all web sites and their components (who would do that, and who would evaluate the results); and who would determine what needs to be fixed and in what order. In addition to addressing these governance challenges, operationally the process would need to be recurring and repeatable to reflect the ever-changing technology and threat environment.

Authentication/Identity (ID) Management

The role of identity authentication is fundamentally important to our national security and economic prosperity. This Administration has taken a keen focus on privacy, security and identity management as a way to increase our security and expand our prosperity in the 21st Century Internet economy. The Department of Commerce plays an important role in this debate with its unique economic perspective. We appreciate the Department's efforts and the thoughtful rollout of numerous listening sessions on these important topics. There are several other government and private sector efforts underway that are examining the role of identity management in society. We would strongly encourage the Department to reach across government and the private sector and incorporate these activities into any further review or programs.

When it comes to identity authentication there are several fundamental key positions that TechAmerica believes should provide the underlying framework of a national strategy.

- **Public-Private Partnership must exist for this to be successful.** The private sector is the consumer and driver of identity authentication and verification. A strong public-private partnership must be developed for the successful implementation of a robust and secure identity framework.

- **There is no One Size Fits All Solution.** Any solution developed must be flexible. The rapid pace of technology innovation combined with the rapidly evolving threat landscape requires agile solutions.
- **All Solutions must be Risk Based.** We can no longer rely on a culture of compliance. The solution must fit the market, business climate and threat landscape.

a. Beyond the measures recommended in the National Strategy for Trusted Identities in Cyberspace, what, if any, federal government support is needed to improve authentication/identity management, controls, mechanisms, and supporting infrastructures?

TechAmerica supports the direction of the NSTIC but believes it is important to also look at the myriad of other ongoing efforts in the public and private sector.[4] It would be helpful to develop an effective mechanism to help agencies work together consistent with the direction of the NSTIC and incorporate many of the specific recommendations and guidelines being developed by other identity management efforts.

[4] Identity management efforts are under way in the Federal Government by the Federal Trade Commission, Federal Communications Commission, Department of Commerce, Federal Identity, Credentialing, and Access Management Working Group, and the National Security Administration to name a few. Additional groups in the private sector are developing guidance, best practices and standards regarding identity management including, but not limited to, the American Bar Association (ABA), National American Security Products Organization (NASPO), and American National Standards Institute (ANSI).

To adequately develop and implement an effective national identity management strategy you must have a strong public private partnership. The private sector is integral to the success of any national strategy. It is important for the NSTIC strategy to recognize and look at other ongoing initiatives.

b. Do the authentication and/or identity management controls employed by commercial organizations or business sectors, in general, provide adequate assurance? If not, what improvements are needed?

The requirements for identity assurance continue to evolve; identity threats and inputs are not static. Passwords are not sustainable in the medium and long term, so new technologies should be constructed and adopted. Private sector organizations need more flexibility to innovate with identity information and new identity technologies. Among government's most important roles is to maintain neutrality in its regulations.

Some industries are ahead of others when it comes to implementing identity management and authentication controls to address security risks. Certain industries are more vulnerable than others. Unfortunately it is often hard to make the ongoing business case (return on investment) to justify the investments needed to keep ahead of the problem. The return on investment for implementing security controls is often not justified until a company is the target of an attack or until there is a business imperative to implement certain controls. In some cases, businesses may not bear the full cost of exposures if they pass on costs to the consumers or their business partners. The business case might be clearer if they bear the full cost, but that information is not always forthcoming. We must focus on the implementation of a layered approach that allows technologies to evolve over time and addresses the risk of the situation.

c. What specific controls and mechanisms should be implemented?

It is not easy to recommend specific controls or mechanism that should be implemented to improve security. The controls and mechanisms needed depend very much on the risk model associated with operating specific enterprises and their interaction with customers and business partners. A one size fits all approach is not appropriate and no single solution can be mandated. A multi-level defense must be used with high risk transactions. In addition, any solution recommended should be consistent with business processes and provide a clear return on investment.

The FFIEC guidance on Multifactor Authentication in the Internet Banking Environment is an example of a multi-layered approach that is not technology specific and works for a particular business community. The guidance set minimum requirements for identity verification online for Internet banking, but did not advocate or mandate a specific technology. This is a solution that has been working in the financial industry but would not necessarily be effective in other business communities.

d. What role should authentication and identity management controls play in a comprehensive set of cybersecurity measures available to commercial organizations?

While large financial companies, telecommunications companies, and credit card issuers tend to have sophisticated identity management controls, smaller organizations often lack the resources to implement advanced authentication and identity management controls. It would be a positive development in cybersecurity if the government could support the development (grant making, purchasing power, etc) of minimum authentication and identity management controls available for smaller organizations. Additionally, the Federal Government should strengthen existing authentication systems (E-Verify, SAVE, Social Security Number Verification) available to the private sector. As the development of enhanced security mechanism for mobile devices flourishes, additional guidance for securing mobile infrastructures may need to be developed.

e. Are the basic infrastructures that underlie the recommended controls and mechanisms already in place?

Partially.

f. What, if any, new tools or technologies for authentication or identity management are available or are being developed that may address these needs?

New technologies and processes exist in the marketplace today that are enhancing identity proofing and authentication. The technology market is constantly changing and it is important to ensure we do not move toward technology mandates or a one size fits all solution.

g. How can the expense associated with improved authentication/identity management controls and mechanisms be justified financially?

Improved authentication reduces fraud, streamlines operational costs, and can make business processes more efficient. An important first step is to concentrate on better education and the development of risk models that can be translated into specific actions for individual enterprises. The cost to implement system should make sense from a return on investment (ROI) perspective. We must have a system people will actually adopt. At the end of the day it is a matter of choice and we have to make it a compelling option.

h. How can the U.S. Government best support improvement of authentication/identity management controls, mechanisms, and supporting infrastructures?

The U.S. government can best support the improvement of authentication/identity management controls by:

- Raising the proofing requirements for government identity documents (birth certificates, passports, driver's licenses);
- Improving government screening and authentication programs and expanding access to some of these programs;
- Deploying the procurement powers of government and allowing State & Local governments access to that purchasing power;
- Funding pilot projects and research;

- Expanding education efforts;
- Providing technical assistance to small and disadvantaged businesses; and
- Developing policies that encourage technological innovation.

i. Is there a continuing need for limited revelation identity systems, or even anonymous identity processes and credentials?

Anonymous identity processes are useful in certain identity contexts, but not all.

j. If so, what would be the potential benefits of wide-scale adoption of limited revelation identity systems or anonymous credentialing from a cybersecurity perspective?

As indicated earlier, there are a number of transactions executed every day which pose minimal or low risk-there is no need to place burdensome identity proofing requirements on transactions that require low levels of assurance. There is a distinction between revelation for identity proofing and revelation for identity authentication. There are instances where you may need anonymization in a highly secure transaction (medical records).

k. What would be the drawbacks?

TechAmerica embraces the value of limited revelation identity systems in certain contexts. However, many government, commercial, and societal activities depend on an appropriately validated or proofed identity. In situations where identity proofing is required, it is necessary to reveal identity information. Government policies that severely restrict ability of proofing organizations to collect personally identifiable information (PII) could seriously impede privacy and security. Systemic restrictions on information sharing could undermine a key objective of a viable identity system which is to promote identity security and prevent fraud. The primary identity verification and fraud prevention systems relied on by America's leading companies today depend on the sharing of identity information.

Unqualified restrictions on data sharing, data retention, and data aggregation would severely impair these and future technologies. We also note that accurate identification of an individual is an important predicate to many key privacy protections such as preventing identity theft, opting -out of unsolicited communications, and granting consumers access to records

I. How might government procurement activities best promote development of a market for more effective authentication tools for use by government agencies and commercial entities?

The government can use its extensive buying power to promote the use of effective authentication tools in the government and commercial market. For the government to be successful at moving the authentication market forward it cannot simply focus on implementation of new federal acquisition regulation (FAR) requirements. Significant training must be done for procurement officials, program managers, and government contractors to expand education of existing requirements, risk models and assessment tools available. The rapid pace of change in the technology environment combined with the constant addition of new government resources requires that education be a key component of any strategy focusing on leveraging the power of the federal budget.

m. Could a private marketplace for "identity brokers" (i.e., organizations that can be trusted to establish identity databases and issue identity credentials adequate for authorizing financial transactions and accessing private sector components of critical infrastructures) fulfill this need effectively?

TechAmerica strongly supports a private marketplace for identity brokers. Many companies are already functioning in this role and have committed significant resources to authentication and proofing for their own business purposes. Both the public and private sector markets are moving toward consolidation and enterprise wide solutions to reap the benefits of economies of scale. Trusted providers of identities could provide a valuable resource for the government and commercial market by alleviating the need for everyone to become identity authentication experts. There are significant legal and economic hurdles to overcome before this market will flourish. But as we move toward standardization and develop a broad risk based set of identity authentication guidelines, we can overcome these hurdles.

n. What would be some of the issues or potential impacts of establishing standards and best practices for private sector identity brokers?

As we move toward establishing standards and best practices for private sector identity brokers we will address issues surrounding privacy, security, and governance. The primary concern would be the need to balance minimum security and privacy standards with flexible enough guidance that would allow for diverse technologies. It will also be important to establish an audit regime that will ensure compliance with established trust frameworks.

o. Should the government establish a program to support the development of technical standards, metrology, test beds, and conformance criteria to take into account user concerns such as how to: (1) improve interoperability; (2) strengthen authentication methods; (3) improve privacy protection through authentication and security protocols; and (4) improve the usability of identity management systems?

The government should establish a program to support the development of technical standards, test beds, and conformance criteria. By establishing these programs the government can begin to address concerns over interoperability, authentication methods, privacy, and usability of identity management systems.

p. What are the privacy issues raised by identity management systems and how should those issues be addressed?

Privacy concerns and the requirements of identity management systems are aligned but do not exactly correspond. While FIPPs (Fair Information Practice Principles) call for the restrictions on the sharing, use, and retention of information, such restrictions on identity proofing organizations could inhibit their ability to verify individuals. Excessive restrictions on data sharing, data retention, and data aggregation would severely impact fraud prevention technologies. We also note such restrictions could impede efforts at identifying online users. Identification of an individual is also an important predicate to many key privacy protections such as preventing identity theft, opting -out of unsolicited communications, and granting consumers access to records. Current efforts are underway to examine this issue at the American Bar Association and we would encourage the Department of Commerce to look at that activity.

q. Are there particular privacy and civil liberties questions raised by government involvement in identity management system design and/or operations?

As with any major government program that handles sensitive personally identifiable information there are elements that must be addressed to garner the public trust. All government identity management programs must build in privacy and security precautions from the start. The public often questions the use of sensitive information by the government.

r. **What other considerations should factor into government's efforts in this area?**

We would encourage the Department of Commerce to focus on what can be achieved in a short time. Developing and implementing an identity trust framework for commercial and government market is a big project that can be easily derailed. The issues are of fundamental important to our national security and economic prosperity, and we would encourage you to focus on short term deliverables.

Global Engagement

Cyberspace is borderless, and, therefore, we encounter global considerations regarding cybersecurity every single day. On the one hand, we cannot stop attacks at our traditional borders, so we need to be engaging with international partners on a sustained basis to leverage partnerships, information, and capabilities to greatest extent possible. On the other hand, our multinational companies, small, medium, and large, are engaging in global commerce and have customers, suppliers, and employees all over the world. As they engage in business in other countries, they encounter challenges to both business operations and cybersecurity efforts.

First, there is a wide range of levels of understanding about the importance of cybersecurity in other countries, customers, and end-users. All present problems for business facilitation and security. As such, there are greatly varying levels of resource in other countries to go to for help for information gathering for greater situational awareness, incident response collaboration, or law enforcement cooperation. In all cases, our companies are hampered by lack of knowledge or coordination points for the quickest possible and appropriate action. Therefore, it is crucial for the U.S. Government to take a leadership role in the global community on cybersecurity to forge important linkages and help build capacity. TechAmerica has long supported the creation of a position of Ambassador for Cybersecurity at the Department of State to coordinate international engagement and strategy. In addition, the U.S. Government's diplomatic efforts in this regard would be well-served by the establishment of a cadre of dedicated "cybersecurity attaches" in U.S. embassies around the world.

Second, our multinational companies often encounter cybersecurity measures by other governments as a market entry or business barrier in the host country. Some countries have tried to demand source code or encryption keys from U.S. companies under the auspices of cybersecurity or national security. In other instances, countries try (and in some cases succeed) to put in place requirements for U.S. companies to operate in the domestic market such as: partnership or technology transfer requirements; legal liability requirements for corporate officers; privacy protection requirements that hamper needed security measures; and prohibitions on transborder data flows. Third, with regard to standards, the best way for the U.S. Government to better encourage the use of global cybersecurity standards and practices outside of the U.S. is to not create its own country specific standards and practices that directly contradict them or indirectly confuse implementation of two sets of standards.

The U.S. Government should continue its participation in existing multilateral, regional, and bilateral forums in which cybersecurity is a subject for dialogue, negotiation, or development. To the greatest extent possible, the U.S. Government should be sure to engage the private sector in the development of policy positions and capacity building/partnership programs in those forums and bilateral relationships in order to develop and cultivate norms for behavior that support greater global cybersecurity. Utilizing existing – and, therefore, established – forums will be more beneficial than trying to create a new body that will have to consider all manner of governance and diplomatic protocols before even beginning to make progress. In addition, utilizing non-negotiating forums such as the Internet Governance Forum, the Forum for Incident Response and Security Teams (FIRST), and other arenas for dialogue would supplement more formal interactions with established partnerships such as those being driven through the Department of Homeland Security's National Cyber Security Division for government-to-government collaboration and cooperation. Among other such opportunities, the Administration can leverage the upcoming Asia Pacific Economic Cooperation (APEC) Leader's Meeting hosted in the U.S. in 2011 to clearly articulate a message that encompasses cybersecurity and innovation.

Product Assurance

A key element to building trust in ICTs and securing the critical infrastructure is driving assurance into the products that make up the infrastructure. While various mechanisms exist today (standards, best practices etc.), many of them can be expanded and improved to greatly further the goal of robust product assurance. Effective security assurance mechanisms can usefully address questions of what threats need to be considered and the degree of confidence that the product actually addresses these threats (e.g., confidence being established via a (licensed) third party validation of software). It may also include verifying that a product not only does what it was designed to do, but also does not do what it was *not* designed to do, (e.g., via insertion of malicious code or corruption of the software in some way). Security assurance typically also addresses lifecycle issues such as the security of the software development environment.

One effective mechanism to demonstrate assurance is through third party validation mechanisms that are licensed and trustworthy. International Standards Organization (ISO) 15408, the International Common Criteria, is the international standard for security assurance and has a robust construct of evaluation labs that are licensed and certified to conduct product reviews. Furthermore, product evaluations done against the Common Criteria are accepted in more than twenty countries.

We recognize that standards and corresponding certifications are only as good as both the input data and the application of the standard or certification. In the case of the Common Criteria, improvements to what elements are evaluated and how the evaluation is conducted is essential to meet the evolving risk environment. Fortunately, many of those improvements are currently underway. However, even a perfect standard and certification will be ineffective if not properly utilized by its customer base. Government can work to close gaps and exceptions in procurement processes that allow acquisition officials to ignore certification and standards for security assurance.

We believe that while certifications are helpful they may be too heavy handed in some cases and thus a lighter, more agile mechanism should also be available to meet different levels of need or risk. We believe that such a mechanism can be founded and grounded in the principles of accountability. Drawing on lessons learned from the disciplines of privacy and data protection, a system by which companies are held accountable for assurance of their products by attesting to the existence of fundamental but critical security policies and processes (including the use of requisite security checking tools) could be put in place. Such policies and processes could include a process for securely developing product that includes the existence of secure processes for product development lifecycles (e.g., coding, review, testing and validation) and evidence that security training and education programs are available and mandatory for engineers and developers as well a broader set of employees that impact product development. Progress to building these accountability criteria and requirements should be a useful glide path to effective Common Criteria modification and implementation. The goal should be to drive global criteria and requirements, as divergent national standards run the risk of creating significant market entry barriers for new technology, and undue compliance complexity for technology intended to be sold worldwide.

Research and Development

TechAmerica has long been a supporter of increased funding for cybersecurity research and development and, importantly, advocates for a coordinated, public-private approach to determining priorities and implementing research and development programs. In June 2009, we testified before Congress that, "the overwhelming bulk of cybersecurity R&D is provided by private sector entities seeking to develop the most innovation solutions to meet the broad market requirements. While having the most innovative security solution available relies on these efforts, there are gaps in cybersecurity capabilities for which there is currently either limited market demand or the lack of market awareness."[5] It is precisely those gaps, particularly in the area of long-term projects that the federal government can try to help fill through providing for tax incentives for private R&D efforts or through direct funding of R&D in academic institutions and in cooperation with the private sector. In all cases, coordination and collaboration is key to ensuring the identification of gaps and priorities and to avoiding duplicative efforts.

[5] TechAmerica testimony before the Subcommittee on Research and Science Education, Committee on Science and Technology, U.S. House of Representatives; June 10, 2009.

For example, through recent coordination and information gathering efforts between industry and government, we have learned that there is little private sector R&D on cyber forensics as it relates to law enforcement evidence trail. This area of investment, then, would appear to be in need of prioritization by government R&D programs to ensure the innovation necessary to align with the critical government mission to analyze cyber incidents. In our testimony, we acknowledged these recent coordination efforts to identify existing projects and needs, but we also recommended that a more formal mechanism be put in place for such input and collaboration: "Such a mechanism should include all the elements of the R&D lifecycle: identification of current and prospective R&D in the industry; determination of the gaps in the market that need to be filled by government efforts, especially as the operations and threat environments continue to evolve; and, where necessary and feasible, joint industry and government collaboration on R&D projects."[6]

Regarding a federal government-sponsored "grand challenge program" designed to draw attention to and promote work on specific technology problems, we believe the verdict on its effectiveness could be mixed. We would suggest that such an effort could be effective if and only if government and industry could collaborate on the development of a concept/program design; if multiple channels for communicating and marketing the program were utilized in a cohesive manner by both government and industry; and if federal funding were attached to the program in some way.

[6] Ibid.

An Incentives Framework

As discussed in various response components above, there are several ways in which incentives could be helpful to fill market gaps and compel organizations to take more action on cybersecurity efforts. Admittedly, addressing an incentives framework is difficult because the field is “new” in the sense of experience and data for metrics and modeling; the stakeholder community is vast and diverse (from enterprise users, to security providers, to non-profit advocacy and education groups, to all manner of end-users); return on investment is hard to measure; and there is no one-size-fits-all solution to all investment challenges. While there is much discussion around how to provide incentives, there is currently no true measure of “adequacy” to address the current risk environment. Different segments of the business community have different challenges to making cybersecurity investments; for examples, small businesses have particular challenges to funding cybersecurity measures – especially when they do not have a real sense of the threats to their network, or the vulnerabilities they can inadvertently introduce into the eco-system by virtue of their connections. Therefore, finding more ways to reach small businesses to provide information about best practices and available resources should be a priority. NCSA already does good work with small business awareness with its industry and government partners, but more can be done to bolster their efforts.

TechAmerica believes there are additional opportunities for injecting positive incentives into the marketplace. As mentioned above, we believe that ways to devise a refundable tax credit for cybersecurity investments should be explored. And, national programs such as broadband deployment and smart grid projects could include cybersecurity considerations to ensure security is infused at the beginning of those efforts. Further, companies that take protective measures, either in steady state or in response to a cyber emergency should not be penalized for their vigilance. For example, pending security and data breach notification legislation provides for safe harbor from notification if protective security measures to render data unreadable and unusable are in place. Similarly, under a reasonable due diligence regime, liability protection should be provided to companies that take extraordinary security measures in order to respond to a cyber emergency, whether directed or approved by designated authorities. Finally, it is important that government refrain from imposing overly burdensome or one-size-fits-all regulations in order to enable them to take protective measures that meet their own risk assessment and management needs.

Conclusion

TechAmerica thanks the Department for creating its Internet Policy Task Force. A committed and focused effort by the Department with regard to the development of the digital economy is welcomed and appreciated. The Department can contribute to the multi-faceted effort to bolster our national cybersecurity posture. TechAmerica looks forward to working with the Department and its government colleagues toward that goal.