CompTIA

September 20, 2010

Diane Honeycutt,
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899.

Dear Ms. Honeycutt,

The Computing Technology Industry Association ("CompTIA") respectfully submits this response to the Department of Commerce's Notice of Inquiry ("NOI"), dated July 28, 2010.[1] CompTIA is a non-profit trade association representing the information technology (IT) industry, and represents over 1,500 IT companies. Our members are at the forefront of innovation and provide a critical backbone that supports broader commerce and job creation. These members include major computer hardware manufacturers, software developers, technology distributors and IT specialists that help organizations integrate and use technology products and services.

CompTIA also develops vendor-neutral certifications, with and for the IT industry, such as: CompTIA A+ , Network+, and Security+ certifications. CompTIA is the largest provider of vendor neutral certifications in the United States and there are currently over 1.5 million holders of CompTIA certifications worldwide.

CompTIA has provided comments on several sections of the NOI. They include:

- Under "Ways to Improve Cybersecurity While Sustaining Innovation," comments that the ever-changing nature of cyber threats requires a more flexible application of the Federal Information Security Management Act's security compliance requirements.

[1] Federal Register/Vol. 75, No. 144/Wednesday, July 28, 2010/Notices, Docket No.: 100721305–0305–01.

- Advocates in favor of a national framework for data breach laws that incorporates a safe harbor program.
- Under the section "An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices," comments that basic IT skills and computer science educational training is the foundation by which private and public sector stakeholders can collaborate to support curriculums aimed at empowering users.
- Supports a federal effort to improve cyber literacy among the general public.

Ways to Improve Cybersecurity While Sustaining Innovation

The Federal Information Security Management Act and Innovation

The United States tech industry has led the world in new and innovative cybersecurity products and services. While this will remain to be true, small and medium-size businesses ("SMB's") are huge innovation drivers in the high tech sector, including in the area of cybersecurity. There are countless examples whereby small and medium size businesses developed new and innovative ways to manage and secure infrastructures against cybersecurity threats. SMB's have a track record for innovating because they tend to be fluid and adept at responding to market needs. SMB's generally do not have the layers of bureaucracy and rigidity often seen in larger more-capitalized companies. This also means that SMB's often have small staffs and budgets and have to learn to act creatively to achieve results within their limited resources.

CompTIA is actively working with policymakers and other stakeholders to eliminate barriers to entry for SMB's so that these businesses can focus their efforts on creating new and innovative products and services for the high tech sector. One area where CompTIA believes there is room for improvement is in the need for consistent cybersecurity standards and practices that are sufficiently flexible to respond to an ever evolving cybersecurity environment. For example, the federal government enacted the Federal Information Security Management Act ("FISMA"). Although FISMA has played a crucial role in ensuring that federal agencies implement and maintain adequate data

security and IT infrastructure protections FISMA has also had the unintended consequence of creating barriers to entry for some SMB's. A similar problem occurred with the initial PCI DSS requirements, which served as a barrier to entry for SMB's, until 2009 when the PCI Security Standards Council revised them for the benefit of small and medium size businesses.

Under FISMA, in order for a managed service provider to offer cybersecurity services to a government agency it must demonstrate that it is FISMA compliant. Once a managed service provider becomes compliant it has a vested interest in maintaining its existing suite of services so that it does not lose or have to reapply for its FISMA certification. Some SMB's argue that FISMA is designed to treat cybersecurity as a static target. For example, once IT hardware has met the security requirements under FISMA it can take months before another security review is once again verified. Meanwhile, in today's cyber environment where security threats occur daily, security professionals must keep up with the ever-evolving environment of cyber threats, software and security updates on a real time basis. The FISMA security compliance approach does not have the requisite flexibility to meet this reality and thus has the unintended consequences of treating identified cyber threats as fixed targets that once identified stand still in time. By comparison, FISMA security compliance approach has the unintended consequences of treating identified cyber threats as fixed targets that once identified stand still in time. As SMB's diligently work to develop new and innovative methods and/or techniques for combating cyber threats, the solutions may never get applied to real world threats if they do not meet the FISMA compliance requirements. As a result, existing managed service providers are inadvertently disincentivized from developing new innovative technological solutions due to the rigid FISMA requirements.

The FISMA model is also largely viewed as a "check mark" certification system without real mechanisms to ensure that a cybersecurity program is sufficiently robust to address the dynamic and continually evolving world of cyber threats. CompTIA believes that a cybersecurity program should be designed to address cybersecurity as a dynamic eco-system. For example, an industry-led cybersecurity accreditation program based on

industry best practices with annual reviews is an approach that balances the need for maintaining the most current security practices while also allowing the flexibility to develop new innovative cybersecurity solutions against cyber threats that are in a perpetual state of evolution. Such an approach creates a meritocracy and incentivizes SMB's and incumbent managed service providers to continuously innovate new and improved cybersecurity solutions. This approach creates a lifecycle whereby those cybersecurity products and services that are superior will rise to the top and will be replaced when new solutions emerge to address ever-evolving cybersecurity threats.

CompTIA supports an improvement to the FISMA model that allows for a more fluid and dynamic compliance approach that encourages and invites ongoing innovation and new cybersecurity products and services.

Data Breach

Another issue undermining the ability of SMB's to effectively compete with larger cybersecurity providers and to have the ability to create new innovative programs comes from the patchwork of data breach laws across the country. A majority of states have enacted a vast array of data breach laws. There is no uniformity amongst them, and in many instances they conflict. SMB's are forced to navigate through individual state data breach requirements to:

- Understand what type of entity is covered by the law,
- Understand under what circumstances is a state notice requirement triggered,
- Determine what is an acceptable form of customer notice,
- Review state laws to understand possible exceptions to a particular notice requirement,
- Identify the correct parties to whom the notices must be provided, and
- Understand whether the state provides for a private right of action.

Companies must work to identify and hire employees with the requisite level of expertise needed to study and understand the patchwork of data breach laws with varying

compliance obligations and penalties. For a company with 10 to 20 employees, navigating through this patchwork of laws can be an expensive, if not impossible, undertaking.

For instance, Arizona's data breach law provides no notice exception and companies must provide customer notice if an unintended party acquires or gains access to a customers personally identifiable information. However, under an Idaho law a company must provide notice to a customer if personally identifiable "information was or is reasonably believed to have been misused." The law provides an exception to the notice requirement if "after a reasonable and prompt investigation, the [company] determines that there is not a reasonable likelihood the personal information has been or will be misused."[2]

Thus, companies may find it easier to simply send out blanket data breach notices whenever there is a suspected or actual data breach of personally identifiable information. The problem with this approach is that over time such notices begin to lose their effectiveness after consumers get accustomed to receiving them. It is similar to political or bulk mail whereby consumers become desensitized to these notices and advertisements so that the letters and/or e-mails containing customer notices go unopened and often disregarded. Nevertheless, SMB's have to incur costs associated with such notices that may not be required because an actual data breach did not actually occur.

In addition, companies are exposed to expensive legal costs as they try to get an assessment of their liability across a patchwork of state legal obligations and liabilities. This patchwork of state data security and breach laws serve as a considerable barrier to entry for small and medium size firms in the area of cybersecurity and data protection.

Eliminating barriers to entry such as the high costs associated with managing conflicting and inconsistent data breach laws helps SMB's stay financially afloat while also creating

[2] Paul M. Schwartz, and Edward J. Janger, Notification of Data Security Breaches, Feb.2, 2007. <www.paulschwartz.net/pdf/datasec_schwartz-janger.pdf>.

a level playing field among small, medium and large companies. This allows all stakeholders to instead focus their efforts on the creation of new and innovative products and services without the overhead costs of maintaining a legal team to manage the current set of conflicting data security and breach laws.

Another barrier to entry for SMB's is the exposure to liability as a result of data breaches. In some states, like California and Louisiana, consumers can file private rights of action for data breaches. These private rights of action may serve as disincentives for large well-capitalized companies, but for the SMB it can be the difference between profitability and bankruptcy without ever establishing fault. The mere initiation of a lawsuit can sink a small company. For this reason, a data security breach and notification law should include a safe harbor provision that provides incentives for companies that implement responsible data security and compliance training programs that render data unusable should it be lost or stolen. Such an approach provides a degree of certainty for businesses that engage in providing cybersecurity products and services while at the same time providing consumers with data protection against cyber fraud, theft, and negligence. This would reduce uncertainty in business security costs and litigation while enhancing incentives for firms to comply with new requirements.

CompTIA supports a national and uniform approach to data breach laws along with safe harbor provisions. Such an approach would help reduce, if not eliminate, barriers to entry for firms focused on providing cybersecurity products and services, while also reducing unnecessary costs for the entire industry.

An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

Basic IT Skills and Computer Sciences Educational Training

CompTIA believes that cybersecurity education is the foundation by which the U.S. government, private and public sector stakeholders should address the increasing vulnerabilities to cyber threats and attacks. U.S. policies should aim to expand life-long education programs in basic IT skills and computer sciences. Education programs should be based on approved curriculum aimed at empowering the user as opposed to programs designed to increase sales or services for profit based educational institutions.

Next, U.S. government agencies should receive sufficient funding for IT literacy and training to set an example for the nation with respect to IT skills and the value of information assurance. These foundational skill sets are imperative for the United States economy and its ability to compete globally, spur job growth and establish global leadership in technological innovation.

For these reasons, CompTIA supports:

- An approach that can generate new jobs to offset job loss in other shrinking industries.
- Aligning laws such as the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and Red Flag Rules, to allow an educational curriculum that is streamlined and simplified because one program can cover several regulations with similar security and privacy requirements.
- Extensive funding and investment for U.S. government R&D (i.e., continued support for U.S. national security labs, academic and research institutions).
- Addressing government wage and hour regulations and its impact on technology companies.
- Government resources for worker training/retraining in IT skills in and out of government (e.g. through the reauthorization of the Workforce Investment Act; assisting government in developing "programs of study" for the transition to electronic health records; or programs such as the DoD Directive 8570.1).
- Government programs to spur technology innovation for job creation and promote life-long re-training for careers in the IT industries.

Leverage Existing Certification and Security Assurance Programs to Ensure a Seamless Ramping Up of Training Programs

CompTIA fully supports and recognizes the immediate need to ramp up certification and security assurance programs to bolster public and private sector efforts to protect against cyber threats. CompTIA also believes that such ramping up efforts should occur in a manner that is not disruptive to existing structures that are currently providing security training to thousands of IT security professionals.

CompTIA as a not-for-profit organization is dedicated to improving technical training; ensuring certifications are relevant and tied to work requirements; and leveraging procurement and human resources to bring the right people and technology to organizations.

As the DOC Task Force moves forward with efforts to identify solutions for fostering cybersecurity and innovation, CompTIA would respectfully recommend that the following guideposts be considered:

- Carefully review empirical evidence to determine the correct approach between knowledge-based and performance-based training. In the absence of an agreed-upon comprehensive body of knowledge, common taxonomy and definition of a cybersecurity professional (all items that the USG is presently seeking to address and an undertaking that CompTIA strongly supports), it is difficult to assess the need and practicality of a performance-based training program. Moreover, thought must be given to capacity to rapidly deploy and execute performance-based testing. Hastily replacing one system for another could result in additional challenges and problems, including significant bottlenecks that would run counter to the national interest.
- Identify multiple sources of information to determine the adequacy (and gaps) of the current IT and cybersecurity certification processes.
- Weigh whether current and proposed solutions support the goal of achieving a

global approach to cybersecurity. CompTIA and other similar organizations are active in the U.S. and global marketplaces and share the belief that cybersecurity must be addressed across national and international boundaries.

- Support an alignment of all certification regimes that effectively meets the needs of professionals who have a thorough understanding of industry best practices, broad knowledge of the cybersecurity field, sound professional judgment, and experience flexible enough to recognize, assess and manage threats in any environment amidst a quickly changing landscape.

In summary, certifying professionals in specific technologies quickly becomes outdated when solutions and processes change with the marketplace; because of this CompTIA supports a continuing education requirement.

As global leaders in the information security and certification community, our goal is to coordinate long-standing expertise in technology, education and certification with the needs of the U.S. government, private, and public sector stakeholders. Through these collaborative efforts we can best ensure that professionals have the necessary expertise in cybersecurity and can effectively serve the broader cybersecurity community, including government agencies, businesses and security professionals.

Raising Awareness (Cybersecurity)

The Federal Government Should Initiate a Cybersecurity Education Campaign

Private sector companies, such as financial institutions, health care providers and retail businesses engaged in the online collection, storage, transmission and management of data containing personally identifiable information are legally obligated and liable for protecting client/customer data. However, if those Internet consumers fail to implement adequate security software on their computers then they could be unsuspecting co-conspirators to cyber crimes. For example, earlier this year the Federal Trade

Commission conducted an investigation uncovering "widespread data breaches at companies, schools and local governments whose employees are swapping music, software and movie files over the Internet. . . [the FTC] sent nearly 100 letters to organizations where information on customers and employees -- including health and financial data and Social Security and driver's license numbers -- leaked through peer-to-peer Web services."[3] The FTC advised these stakeholders that such data breaches could lead to "identity fraud or theft." This is just one of countless examples where Internet users fail to use proper cybersecurity practices leading to cyber theft and fraud. Every year there are also countless numbers of consumers who become victims to identity fraud and theft through phishing scams whereby consumers disclose proprietary information via e-mail. Nevertheless, the costs associated with cyber theft and fraud is ultimately passed on to the consumers and it accounts for billions of dollars lost from the U.S. gross domestic product.

The American public has become so dependent on the Internet that the US government should undertake a nationwide public education and awareness campaign designed to educate the public about the dangers of cybersecurity and suggest simple solutions individuals can take to protect sensitive information. The U.S. government has demonstrated its ability to lead effective educational campaigns in the past.

CompTIA believes that it is time for the federal government to partner with non-profit organizations to create and launch a nationwide cyber education campaign to educate students and consumers about the threats to their personal information and simple measures they can take to prevent crimes from occurring in the first place.

Closing Remarks

CompTIA applauds the Department of Commerce for its leadership in undertaking the very important task of identifying ways to improve cybersecurity while also fostering

[3] http://www.washingtonpost.com/wp-dyn/content/article/2010/02/22/AR2010022204889.html?hpid=sec-tech

innovation. As a not-for-profit organization that represents a cross-section of over 1,500 IT focused businesses CompTIA looks forward to continued collaboration and engagement with federal agencies, such as the Department of Commerce, and its National Institute of Standards and Technology to develop solutions to the important issues raised in the NOI.