SIIA Accelerating Innovation in Technology, Data & Media

202.289.7442 1090 Vermont Ave NW Sixth Floor
www.siia.net Washington DC 20005-4905

Submitted via email: cybercommission@nist.gov

September 9, 2016

Nakia Grayson
Computer Security Division, Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: Input to the Commission on Enhancing National Cybersecurity

Dear Ms. Grayson,

On behalf of the members of the Software & Information Industry Association (SIIA), thank you for the opportunity to provide comments to inform the Commission on Enhancing National Cybersecurity (Commission) about current and future states of cybersecurity in the digital economy. SIIA also thanks the National Institute of Standards and Technology (NIST) for its leadership on cybersecurity and support of the Commission.

SIIA is the principal trade association for the software and digital information industries. The more than 700 software companies, data and analytics firms, information service companies, and digital publishers that make up our membership serve nearly every segment of society, including business, education, government, healthcare and consumers. As leaders in the global market for software and information products and services, they are drivers of innovation and economic strength—software alone contributes $425 billion to the U.S. economy and directly employs 2.5 million workers and supports millions of other jobs.[1]

National and economic security of the United States depends on strong cybersecurity protections, including but not limited to the reliable function of critical infrastructure. Yet cyber threats continue to increase at a dramatic pace. Effective cybersecurity risk-management therefore is imperative for all organizations, both public and private.

SIIA and its members share the Obama Administration's critical priority to enhance the cybersecurity of our Nation. We are dedicated to maintaining and expanding the partnership between the private sector and the government to address our collective cybersecurity challenges. To that end, we have spent much time over the last several years working closely

[1] The U.S. Software Industry: An Engine for Economic Growth and Employment; SIIA; 2014.

with administration officials and congressional leaders to promote flexible, risk-based policies to address the increasing cybersecurity challenges. Please find below recommendations which address many of the key issues you have identified, and answers to many of the specific questions raised in the request for information.[2]

Retain Strong Commitment to NIST Cybersecurity Framework with Minimal Changes

Since its inception more than two years ago, the NIST Framework for Improving Critical Infrastructure Cybersecurity has proven to be an effective, flexible approach to cybersecurity, because it recommends a suite of standards, guidance and best practices, rather than providing a prescriptive set of step-by-step requirements for entities. Consistent with many other recent initiatives where NIST has played a convening role among technologists, experts and industry leaders, NIST should be commended for its comprehensive accomplishment of producing, and now working to update the Framework.

The breadth and flexibility of this approach has gained strong support from policymakers, technologists and entities increasingly relying on the document's guidance—support for the framework has been substantial, as demonstrated by participation and feedback from the many workshops and the feedback received by NIST earlier this year.[3]

SIIA strongly supports efforts to maintain and expand the partnership between the private sector and the government to address our collective cybersecurity challenges. We urge the Cybersecurity Commission to promote a flexible, voluntary approach to developing cybersecurity best practices, consistent with the NIST Cybersecurity Framework and the efforts identified by the Obama Administration's 2011 Green Paper.[4]

Promote the NIST Cybersecurity Framework for International Adoption

In seeking to enhance cybersecurity of the public and private sectors, collective efforts should reflect the borderless and interconnected nature of the global internet. Like NIST and the U.S. Government, governments around the world are examining potential policy reforms to address rapidly evolving cybersecurity challenges. In the absence of global norms, it is likely that a patchwork of inconsistent international cybersecurity mandates will evolve over the next decade. This patchwork threatens to dramatically impede global cyber-preparedness, and therefore should be avoided.

To that end, we appreciate the efforts of NIST to engage with foreign governments to promote the Framework, and we urge NIST to work closely with the State Department's Office of the Coordinator for Cyber Issues (S/CCI). As the Administration's chief coordinator for global diplomatic engagement on cyber issues, the S/CCI is uniquely positioned to engage with our

[2] Information on Current and Future States of Cybersecurity in the Digital Economy; NIST; August 10, 2016.

[3] Analysis of Cybersecurity Framework RFI Responses; NIST; March 24, 2016.

[4] Cybersecurity, Innovation and the Internet Economy, NIST, 2011.

international partners to actively promote the Framework as a model for cybersecurity policy development.

Additionally, SIIA recommends that NIST also consider submitting the Framework as an international standard. Recognition by a standards organization would bolster the Framework's credibility among international constituencies and help to ensure that other countries considering cybersecurity regulations opt for a standards based approach.

SIIA encourages the Commission to prioritize U.S. Government leadership to work with international partners in search of opportunities for stakeholders to participate in multinational discussions which are stakeholder driven.

Align Federal Cybersecurity Requirements with the NIST Cybersecurity Framework

A majority of technology companies service both the public and private sectors. However, there is an extensive set of cybersecurity requirements maintained by the U.S. Government, which often do not align effectively with the Cybersecurity Framework. Therefore, aligning Federal Information Security Management Act requirements with the Framework subcategories, and mapping these requirements to other global standards referenced in the Framework, is a critical priority. This alignment will better enable vendors to comply with federal requirements and compete in the public and private sector information security marketplaces, driving further innovation and improving security capabilities. Indeed, identifying and reducing the cyber regulatory burden on the business community is a key objective of both the 2013 Cybersecurity Executive Order (EO 13636)[5] on strengthening critical infrastructure and the Cybersecurity Enhancement Act of 2014.[6]

SIIA urges the Commission to encourage continued dialogue between NIST and its interagency partners to drive alignment of cybersecurity requirements for Federal information systems with the cybersecurity outcomes of the Framework. SIIA also encourage the Commission to prioritize the need for the next administration to engage in a dialogue with various key industry groups and entities to expand voluntary partnerships to bolster cybersecurity in and out of the Federal Government.

Reinforce the Need for a Multi-layered Approach for Federal Data Security

As one of the largest holders of personally identifiable information (PII), as well as classified, sensitive and related critical information, the U.S. Government must enhance data security amidst growing cyber threats. Currently, federal data is often stored in legacy information systems and transmitted by email or moved from location to location using portable storage devices. This reality increases the potential exposure or loss of sensitive data.

In order to effectively protect this sensitive data, the U.S. Government needs to embrace a multi-layered approach, implementing what is often referred to as "data-centric security."

[5] Executive Order -- Improving Critical Infrastructure Cybersecurity; President Obama; Feb. 12, 2013.

[6] See Cybersecurity Enhancement Act of 2014 (S. 1353, PL 113-274).

Data-centric security refers to the act of ensuring that data remains secure wherever it travels or is stored. Working together, various technologies form a layer of security inside a firewall that can better protect sensitive government data, even in many cases where a hacker is able to breach the agency's perimeter security. For instance, attribute-based access control (ABAC), Digital Rights Management (DRM), Document Analytics and Digital Signature are all increasingly common security technologies that should be leveraged by the U.S. Government. In addition to adding another critical layer of security, these technologies can enable the government to monitor and control the data, assisting law enforcement and security personnel to track stolen data.

Recognizing this reality, recent White House cybersecurity policies and federal legislation highlight the need for a multi-layered approach to better protect the Government's sensitive data. For instance, OMB Circular A-130, White House Cyber Security National Action Plan (CNAP), and the Cybersecurity Strategy and Implementation Plan (CSIP) all support this approach. Specifically, the recently revised OMB Circular A-130 also establishes minimum safeguarding of federal information requirements and best practices that the commercial and government cybersecurity enterprise should follow:

- *Implement data-level protection and access controls to ensure the security of and access to Federal Information;*
- *Continuously monitor, log, and audit the execution of information systems functions by privileged users to detects misuse and reduce risk from insider threats;*
- *Encrypt all FIPS 199 moderate-impact and high impact information at rest and in transit;*
- *Implement processes to support use of digital signatures for employees and contractors; and*
- *Implement a policy of separation of duties…..to reduce risk of malicious activity without collusion*.[7]

The CNAP and CSIP and congressional legislation provide similar guidance, calling for agencies to, "protect high value assets and sensitive information" and to "encrypt or otherwise render indecipherable to unauthorized users the data…stored on or transiting agency information systems," within the next year.[8] Additionally, the Cybersecurity Act of 2015 includes "information security management practices" such as "digital rights management" as a capability that federal agencies must report on utilizing "to monitor and detect exfiltration and other threats."[9]

The Commission should underscore the value of these technologies for use in the U.S. Government, consistent with the recent legislation and administrative guidance.

[7] Circular No. A-130, Managing Information as a Strategic Resource; OMB; July 28, 2016.

[8] See the Cybersecurity National Action Plan; White House; Feb. 9, 2016; and the Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government; White House; Oct. 30, 2015.

[9] See Section 406 of the Cybersecurity Act of 2015 (H.R. 2029, PL 114-113)

Encourage Further Progress for Cyber Threat Information Sharing

SIIA applauds Congress and President Obama for enacting the Cybersecurity Information Sharing Act of 2015 (CISA). This critical legislation established a voluntary information-sharing framework, intended to strengthen businesses' protection and resilience against cyberattacks. The law gives businesses legal certainty that they have safe harbor against frivolous lawsuits when freely sharing and receiving cyber threat indicators (CTIs) and defensive measures (DMs) in real time and taking actions to mitigate cyberattacks.

CISA empowers the use of Information Sharing and Analysis Centers (ISACs) or Information-Sharing and Analysis Organizations (ISAOs), critical centralized resources for gathering information on cyber threats within particular industries, and enabling sharing of this information between the public and private sectors. However, broad participation in these entities may take some time. It is likely that information sharing practices will start small, and in some cases will be done through informal channels and voluntary networks outside of ISAOs/ASACs. Many organizations, particularly small and medium-sized entities, are not likely to have the financial and personnel resources to establish an information sharing program or to join an ISAC or ISAO. Therefore, initial participation in these initiatives should not be used to gauge the effectiveness of this framework.

While industry leaders and industry groups will play a leading role in encouraging company information sharing, either informally or through ISAOs/ISACs, this is also a critical role of government. Industry participants must have knowledge and confidence in the system, so it is also imperative that cybersecurity policy leaders continue to educate industry and encourage entities to join an ISAO or an ISAC, and to take advantage of the CISA framework as appropriate.

Promote Authentication and Fraud Prevention Efforts

Effective authentication and the ability to combat online fraud are both critical cybersecurity objectives to ensure continued success of the digital economy. SIIA strongly supports initiatives—including but not limited to multistakeholder initiatives—and policies focused on authentication techniques, voluntary policies and practices to prevent fraud and identity theft.

At a time when Americans are performing increasingly important functions online—including managing bank accounts, shopping, paying bills and handling medical records—it is imperative that our collective cybersecurity objectives include efforts to help protect the most vulnerable: consumers who can easily fall victim to attacks that leave personal data vulnerable to hackers and cyber-criminals. Once a consumer's data is compromised, it can then be used to wreak havoc, including identity theft, take-over of online accounts, and to commit fraud. In many cases, the end result is considerable financial harm to the consumer, and sometimes the entity providing the service.

The Federal Government should look to engage the private sector in building public private partnerships, where possible, to maximize effectiveness of these efforts. NIST is well suited to engage in these efforts, as are the Department of Commerce (DOC) NTIA, and other federal agencies that work closely with the private sector and other key stakeholders.

The IRS Security Summit provides an excellent example of how public-private partnerships can yield demonstrable results in the effort to strengthen cybersecurity on a national level. The initiative brought together leaders from the IRS and state tax agencies along with executives from the private-sector tax software industry in an effective effort to combat identity theft tax fraud. This partnership has been ongoing for the past 18 months, and thus far it has led to new password requirements for DIY filers, information sharing between the IRS and tax software providers to help spot fraudulent activity, and regular security reviews and reports to help the IRS and states find and address new fraud schemes.

Based on the IRS' own data, the first year of this partnership led to substantial progress against tax refund fraud, including the prevention of $1.1 billion worth of fraudulent returns and suspension of 36,000 other returns pending review.[10] The IRS has also reported a 48 percent drop in identity theft reports on the IRS Identity Theft Assistance Service, and a 66 percent drop in financial institution reports of suspicious refunds. SIIA strongly supports continuation of this initiative and other similar public-private partnerships to enhance authentication and fight online fraud.

SIIA encourages the Commission to recognize the critical role of authentication, and the value of public private partnerships and multistakeholder forums to engage a broad group of stakeholders to change the nature of authentication, bringing it into the 21st Century.

Enhance Public Awareness and Education

In addition to the aforementioned authentication priorities, there are other closely related areas where the Government can play a key role in promoting public awareness of good cyber hygiene and educating small and medium-sized entities, and end users.

Particularly, SIIA urges the Commission to promote further awareness and consensus around best practices around botnet and malware mitigation.

- ***Botnet Mitigation*** – The software industry is at the forefront of the fight against botnets and other forms of Internet security threats, including notification efforts for users of computers and routers infected, and in the provision of tools for consumers and businesses to keep their systems free of infections and to remove malware and botnets from their infected systems.

  SIIA is committed to addressing botnet security threats by working collaboratively with the government and by promoting the work of our members. We participated in the DOC-led Industry Botnet Group ("IBG"), a multistakeholder process convened in 2011

[10] See Security Summit Reviews 2016; IRS; June 26, 2016.

which produced Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace. These Principles provided a positive step forward, calling on Internet participants to coordinate and communicate with each other and voluntarily work to fight the effectiveness of botnets across the botnet lifecycle.

However, there is much work still to be done, as botnets remain a major challenge to our Nation's cybersecurity and digital commerce, continuing to infect computers, threatening the trust and confidence of online users and undermining the efficiencies and economic growth spurred by the Internet. Industry and government must continue to work together to further combat these challenges. SIIA believes that the DOC, particularly through the leadership of NTIA and NIST, could provide a valuable coordinating function at this time.

- ***Malware Mitigation/Malvertising*** – Malware is a closely-associated threat, as it is often a key enabler or root cause of botnets. Malware therefore remains one of the greatest cybersecurity challenges to consumers and businesses, particularly small and medium-sized businesses with fewer resources to protect themselves. Not only are there the challenges associated with protecting systems from malware, but once a system is compromised, organizations need to improve the ability to minimize their damage. Because today's malware uses multiple vectors to spread including infecting file shares and brute-forcing weak passwords, organizations need to implement comprehensive information security policies and procedures that address all areas of potential compromise and vectors of attack. Unfortunately, even encrypted web transactions may not protect sensitive information if the user's computer has been infected.

  In 2012, the U.S. Computer Emergency Readiness Team (US-CERT) identified that malware advanced from mere disrupting services to well organized schemes actively seeking financial gain. Since then, attackers using malware have become even more adept at circumventing traditional defenses such as anti-virus software and firewalls.

  Despite the persistent growth of malware and its destructive impact, most consumers and small businesses are still not well educated and remain at risk. SIIA believes that much additional work could be done by the Government to continue promoting voluntary guidelines, procedures and best practices to combat the threat posed by malware and "malvertising." The threat of malware has been rapidly spreading on mobile devices as well; global smartphone infections have increased by nearly 100 percent in the first six months of 2016, compared to the second half of 2015.[11]

[11] Nokia Threat Intelligence Report – H1 2016; Nokia Threat Intelligence Laboratories; 2016.

Promote a Framework to Secure the Internet of Things

An Internet of Things (IoT) without adequate security would be an IoT of little benefit. Therefore, IoT security challenges must be adequately addressed. Market forces will continue to play a critical role to promote the advancement of risk-based security frameworks and commonly accepted standards for connected devices and new IoT services, and government oversight can help enforce reasonable security, even as industry standards progress over time.

While history over the last two decades has demonstrated the challenge to continually update public policies to keep pace with technology, this is likely to be even more so in the years ahead. The IoT will continue to rapidly evolve over the next couple decades, leading to what many have termed, the "Internet of Everything," where Internet connectivity is ubiquitous and devices will regularly communicate with each other as part of their basic functionality.

With such a dynamic technological environment, new regulations run the risk of stifling burgeoning innovation that holds the promise of transforming the way we work, communicate, learn and live our lives. Instead, industry best practices and self-regulatory codes of conduct can provide more flexibility to evolve and adapt over time with technology and user preferences and expectations. For instance, voluntary but enforceable codes can be used to establish frameworks that enable individuals to associate usage preferences with connected devices, indicating to other devices how information collected from individuals' devices may be used. Well-behaved companies will typically inform users of their devices regarding the information collected by the device and how it is used.

IoT device-makers and service providers must provide reasonable security measures. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the device's functionality and the costs of remedying the security vulnerabilities. Security best practices will not apply uniformly across all uses of all IoT devices. Rather industry-specific codes are more likely to be properly designed to meet the specific security challenges in each economic sector. Uniform government regulations could not be effectively applied either.

Privacy and security "by design," or the practice of building privacy and security into devices early in the design cycle of a technology rather than as an afterthought, are critical elements to the IoT. Security risk assessments, continuous monitoring, the use of strong encryption for sensitive information or where there is considerable security risk, security defaults and security testing prior to product launches are all elements that should be considered in a security-by-design approach. These can be used as the basis for codes of conduct to guide various IoT industry segments.

Policymakers should consider ways to incent the combination of privacy and security by design techniques and adherence to industry codes of conduct and best practices which establish responsible data principles, rather than mandating such practices through overly rigid legislative or regulatory approaches. Together, industry-driven best practices and responsible data stewardship practices—both of which can be enforced under current law—can create an effective responsible data use framework that balances privacy and security with innovation, and account appropriately for risk.

Develop a Cyber Workforce

Maintaining effective cybersecurity in the 21st Century is dependent on our Nation's ability to increase the number of skilled cybersecurity professionals. To that end, SIIA supports the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework. SIIA encourages the Commission to consider how for the development of a cybersecurity workforce that should be leveraged by the Framework.

Conclusion

Thank you again for the opportunity to provide comments to inform the Commission on Enhancing National Cybersecurity (Commission) about current and future states of cybersecurity in the digital economy. If you have questions or for more information, please contact David LeDuc, SIIA's Senior Director for Public Policy, at dleduc@siia.net or (202) 789-4443.

Sincerely,

Ken Wasch

Ken Wasch
President