From: **David LeDuc**
Date: Sat, Apr 8, 2017 at 3:18 PM
Subject: SIIA Comments to Cybersecurity Framework Draft Version 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Thank you for the opportunity to provide comments on the Cybersecurity Framework Draft Version 1.1 (Revised Framework). Please find enclosed comments from the Software & Information Industry Association.

David LeDuc | Senior Director, Public Policy

Software & Information Industry Association

www.siia.net

[Attachment Copied Below]

Submitted via email: cyberframework@nist.gov

April 10, 2017

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

RE: SIIA Comments Re: Cybersecurity Framework Draft Version 1.1

Dear Adam,

On behalf of the Software & Information Industry Association (SIIA), thank you for the opportunity to provide comments on the Cybersecurity Framework Draft Version 1.1 (Revised Framework). SIIA also thanks the National Institute of Standards and Technology (NIST) for its continued leadership in working with industry and security experts to develop and promote the Cybersecurity Framework, dating back to the beginning of this important initiative in 2013.

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 maintain a 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 with administration officials and congressional leaders to promote flexible, risk-based policies to address the increasing cybersecurity challenges.

---

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

Since its publication three years ago, the NIST Cybersecurity Framework has proven to provide 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, we commend NIST 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 reflected by participation at the workshops and the feedback provided over the last year.[2]

SIIA strongly supports efforts to maintain and expand the partnership between the private sector and the government to address our collective cybersecurity challenges. The original Framework and this revised version are critical elements of NIST's efforts to continue coordinating industry as directed by the Cybersecurity Enhancement Act of 2014. Below are comments in response to two critical additions proposed in the Draft Framework: Metrics and Measurements, and Supply Chain Risk Management, and to guide NIST as it finalizes and continues working to promote broader adoption of the Framework. Please find below reactions to the Revised Framework, and recommendations about how to maximize its broad adoption and overall effectiveness.

Cyber Supply Chain Risk Management

SIIA agrees with the Revised Framework's conclusion that many organizations may not understand the full implications of cyber supply chain risks, or they may not have the appropriate processes in place to identify, assess and mitigate their supply chain risks. To that end, we support the effort by NIST to build this into the Revised Framework. We also agree with the identification of this as a cybersecurity element that occurs at some, but not all levels of the organization, and one that is not a reoccurring or repeatable threat over time.

Encouraging entities to adopt and implement policies, processes and procedures to address supply chain risk, such as ensuring appropriate agreements are in place to establish baseline requirements for suppliers and partners, is a useful addition to the Framework. The Revised Framework's recommendations in this area are consistent with the widely-shared objective to encourage organizations to leverage mutually recognized international standards and agreements that enable ICT manufacturers to build products and sell them globally. Conversely, prescriptive national cyber supply chain mandates, particularly creating a U.S.-specific approach, could pose a fundamental risk to international competitiveness of U.S. ICT vendors. SIIA continues to support policies that promote globally recognized standards and facilitate trade, while also allowing for effective cyber risk management.

---

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

Cybersecurity Metrics and Measurements

The Revised Framework appropriately identifies that effective measurement can provide a basis for trusted relationships, and that over time, it can help organizations understand and convey meaningful risk information to partners and customers. The Revised Framework identifies the need to use both "metrics" and "measures," comprising both quantitative and qualitative approaches to assessing the impact of cybersecurity practices.

SIIA believes that measurement can sometimes be effective to determine whether or not a business objective is achieved. However, it is more practical, and ultimately more important for purposes of enhancing cybersecurity, to assess the potential for future threats and/or failures to achieve future business goals. As the Revised Framework identifies, the effect of cybersecurity outcomes on a business objective may often be unclear. Therefore, SIIA cautions NIST that in seeking to measure beneficial cybersecurity outcomes, private sector organizations should not be compelled to disclose these metrics to third parties, either public or private entities.

SIIA also agrees with NIST that more work should be performed linking metrics to beneficial outcomes. Given the lack of standards surrounding cybersecurity measurements, SIIA recommends this as an area where NIST could provide substantial additional value.

Promotion of the NIST Cybersecurity Framework for International Adoption

This element point is partially outside the scope of this revision process. However, the proposed revision plays a critical role to the extent that it continues to 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. Such a patchwork threatens to dramatically impede global cyber-preparedness and should be avoided.

Therefore, we appreciate that the Revised Framework avoids catering to specific national standards, particularly in the area of supply chain risk management. This approach will enable continued efforts by NIST and other organizations, both public and private, to engage with foreign governments to promote the Framework. 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 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.

Conclusion

Thank you again for the opportunity to provide comments on the Revised Framework. If you have questions or for more information, please contact David LeDuc, SIIA's Senior Director for Public Policy.

Sincerely,

Ken Wasch
President