Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

December 13, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Dear Mr. Sedgewick,

The Software & Information Industry Association (SIIA) and our members are dedicated to maintaining and expanding the partnership between the private sector and the government to address our collective cybersecurity challenges. To that end, I thank the National Institute of Standards and Technology (NIST) for collaborating with industry in the development of the Preliminary Cybersecurity Framework, and for the opportunity to provide comments on this document.

SIIA has appreciated the opportunity to work closely with NIST across a wide range of initiatives to facilitate and support the development of voluntary, industry-led standards, and we support NIST's leadership in this effort to identify cybersecurity standards and best practices for critical infrastructure. Further, we support the Framework's role to provide guidance to organizations on managing cybersecurity risk, and its commitment to existing consensus standards, guidance and best practices.

SIIA believes that the development of this framework is a critical step to enhancing the protection of our Nation's critical infrastructure, and we remain strongly convinced that a regulatory approach seeking to cover a broad, rapidly-evolving cross-section of industry would have the unintended consequence of slowing technological innovation and limit our collective cybersecurity preparedness. Therefore, we look forward to continuing to work with NIST and federal agencies as they implement the framework, including the identification of additional voluntary consensus standards and processes to encourage adoption of the Framework and applicable standards.

With respect to the privacy methodology, SIIA urges NIST to ensure that the Framework remains appropriately focused on mitigating impacts of cybersecurity practices and associated information security measures or controls on privacy, as directed by the

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

President's Executive Order (EO).[1] As currently drafted, the Framework presents a comprehensive privacy methodology that creates a privacy and data security protection framework which is both overly-broad in scope and too prescriptive in identifying practices and procedures that do not meet the EO's mandate of enjoying consensus industry standards.

While privacy must be considered in the context of cybersecurity practices in many cases, as noted in the Preliminary Framework, not all cybersecurity measures or controls have privacy implications. Yet, the Preliminary Framework attempts to map privacy practices across the broad range of cybersecurity activities.

In addition to more narrowly tailoring the Framework to correspond with appropriate cybersecurity controls, the Framework should more effectively adhere to its critical objective to rely on consensus standards and industry best practices. As stated in the Preliminary Framework, "There are few identifiable standards or best practices to mitigate the impact of cybersecurity activities on individuals' privacy."[2] The Preliminary Framework's relies on Fair Information Practice Principles (FIPPS) as if it is obvious or easy to apply these principles in a cybersecurity context. There is no consensus, however, among practitioners or policymakers in industry or government as to how to bring FIPPs to bear on the question of protecting privacy in a cybersecurity context. The overall result is that this set of recommended practices is likely to discourage private sector entities from fully embracing the Framework. As an alternative, the emphasis on privacy should reflect the lack of consensus standards and the need for an evolving, flexible framework that keeps pace with rapid IT innovation.

Finally, protection of civil liberties applies only in a narrow element of this Framework, as these considerations potentially arise through the government cybersecurity processes or possible government obligations on entities working in collaboration with the government. The Framework should be clear to recognize the distinction between privacy and civil liberties, and how they may or may not pertain to private sector entities.

With the objectives of creating an effective framework that can be broadly adopted by private sector providers, SIIA supports the Alternative Methodology to Protect Privacy for a Cybersecurity Programs, submitted by Harriet Pearson, which represents a consensus approach to more effectively tailor the privacy objectives of the EO.[3] In considering an organization's overall governance of cybersecurity risk, the proposal identifies four key functions where organizations should evaluate and identify privacy threats, and consider

---

[1] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.
[2] P. 39
[3] Comments from Harrier Pearson, Hogan and Lovells, December 5, 2013.

processes to address these threats: access control measures, cybersecurity monitoring, cyber threat information sharing and cybersecurity awareness and training. SIIA concurs that these are the critical functions where the Framework should place emphasis for privacy considerations.

As noted by this proposal, securing personal information is an element of both cybersecurity as well as privacy programs overall. This alternative, whether included in the Framework directly as part of the core or as an appendix, does not extend or apply commercial data practices or activities outside the cybersecurity context.

Again, thank you for the opportunity to provide input in the development of the Preliminary Cybersecurity Framework, and the opportunity to provide comments on this document. We look forward to continuing to work with you towards the creation of a final Cybersecurity Framework.

Sincerely,

Ken Wasch
President