TechAmerica
WHERE THE FUTURE BEGINS

TechAmerica.org

TechAmerica
601 Pennsylvania Avenue, NW
Suite 600, North Building
Washington, DC 20004
P 202.682.9110

December 13, 2013

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

Subject: Preliminary Cybersecurity Framework Comments

TechAmerica, the leading technology trade association, appreciates the opportunity to comment on the NIST Cybersecurity Framework.

TechAmerica strongly supports the effort of the Administration to fill in cyber security gaps, though we believe that legislation is still necessary to fill in areas that the Executive Order (E.O.) does not reach, such as information sharing and liability protection.

TechAmerica generally supports the E.O. and the efforts of NIST to implement the E.O. We are also very supportive of the open and transparent process that NIST has engaged in to ensure stakeholder participation in the process.

The one area where we have significant concerns with the Framework is in the area of privacy, and particularly Appendix B.

While there may be some laudable privacy goals contained in Appendix B, TechAmerica is concerned that these broad provisions, such as access and correction rights, limitations on use of data, and other requirements that are not relevant to cyber security, will slow the adoption of an otherwise necessary and important initiative. In particular, we believe that the application of FIPPs is inappropriate in the cyber security context, given the lack of consensus around standards of application to many of the entities that may end up being covered. We are also concerned that the overly broad privacy provisions may bleed into other areas that are well outside what is necessary for cyber security.

Specifically, we have concerns about the Governance Section, and its discussion of "policies and procedures that address privacy or PII management practices," particularly as they relate to cyber security. Instead, we encourage NIST to adopt the methodology proposed by Hogan Lovells in

TechAmerica
601 Pennsylvania Avenue, NW
Suite 600, North Building
Washington, DC 20004
P 202.682.9110

its comments on the Framework,[1] which can be inserted either immediately before or after Appendix A. This methodology appropriately focuses on the core privacy provisions necessary to help achieve a strong cyber security regime, while eliminating privacy provisions not directly implicated by cyber security activities.

In particular, we would argue that the cyber security framework is not the appropriate time or place to attempt to make privacy policy beyond what is necessary for cyber security. First of all, it is not appropriate in this context – if NIST wants to address privacy issues in a multi-stakeholder context, it has already established a model, and should use that more appropriate venue to address privacy issues.

Additionally, while cyber security and privacy considerations overlap in some areas, it is important to address those issues within their respective contexts. Intertwining those issues may limit the ability of companies to have the right people or expertise to address these issues in the correct context. Further, combining the issues may force companies to make trade-offs between unrelated privacy provisions and cyber issues that may be different than if they were considered separately.

We would also urge NIST to clarify that the privacy methodology only applies to critical infrastructure. This would mirror Section 7 of the EO, which defines the scope of the Framework's application as "cyber risks to critical infrastructure"; same for the first paragraph of the Framework, which refers to "critical infrastructure." Specifically, NIST should be explicit that the principles articulated there aren't intended to be applied on a broader basis, given the variety of contexts in which information is used outside of critical infrastructure.

NIST should also ensure that organizations have the requisite flexibility to develop policies and practices that are appropriate to their respective business models.

Legislation Is Still Necessary

There are still several gaps in the cyber security framework that the Administration's welcome Executive Order cannot fill. To meet those needs, legislation is necessary.

[1] The methodology submitted by Hogan Lovell's is available at http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.

TechAmerica
WHERE THE FUTURE BEGINS

TechAmerica.org

TechAmerica
601 Pennsylvania Avenue, NW
Suite 600, North Building
Washington, DC 20004
P 202.682.9110

Specifically, TechAmerica continues to urge Congress to enact legislation which enables information sharing and liability protection, and we call on Congress, and particularly the Senate, to pass H.R. 624, the Cyber Intelligence Sharing and Protection Act, (CISPA), so that the business community will have all of the tools necessary to effectively deal with cybersecurity threats.

TechAmerica sincerely appreciates the opportunity to participate in these important discussions, and we look forward to continuing our dialogue with NIST on these important matters.

Please contact Joseph Rubin to discuss these matters in more detail at 202 557-4180, or Joe.Rubin@techamerica.org.