TechAmerica
Powered by CompTIA

1001 19th St., North, Suite 2000
Arlington, VA 22209
P: 202.682.9110 F: 202.682.9111

TechAmerica.org
CompTIA.org

October 10, 2014

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

RE: TechAmerica comments in response to NIST RFI: "Experience with the Framework for Improving Critical Infrastructure Cybersecurity"

Dear Ms. Honeycutt:

On behalf of the members of TechAmerica, the public sector and public policy department of CompTIA (TechAmerica)[1], I am pleased to present our comments to the National Institute of Standards and Technologies (NIST) Request for Information (RFI) on "Experience with the Framework for Improving Critical Infrastructure Cybersecurity."

The threats to our nation's critical infrastructure are continually growing, and our capacity as a nation to protect US critical infrastructure from cyber attacks must remain at the forefront of governing. There is no doubt that cyber threats are constantly plaguing both private sector and government networks. From individual hackers, to criminal rings, to nation-states, to terrorists, America's adversaries aim to disrupt or destroy our information infrastructure.

TechAmerica and its diverse body of members are dedicated to maintaining and expanding the partnership between the private sector and the government to address our nation's cybersecurity preparedness. Our membership represents large, medium, and small technology companies that together help to keep the United States at the forefront of technological innovation. Our members are the job creators and innovators that develop new technologies that keep Americans safe from threats internal and overseas. As such, we have a unique perspective on the NIST Framework for Improving Critical Infrastructure Cybersecurity (Framework), and the awareness, usage, and experience with the Framework varies greatly. Some of our members were and continue to be deeply involved in the crafting and shaping of the Framework, and some have very little knowledge of the Framework and its implications for their business.

[1] TechAmerica advocates before decision-makers at the state, federal and international levels of government. Representing technology companies of all sizes, TechAmerica is committed to expanding market opportunities and driving the competitiveness of the U.S. technology industry around the world. With offices on Capitol Hill and in Northern Virginia, Silicon Valley and Europe, as well as regional offices around the U.S., we deliver our members top-tier business intelligence and networking opportunities on a global scale. Learn more about TechAmerica at www.techamerica.org or follow us on Facebook, Twitter or LinkedIn.

TechAmerica
Powered by CompTIA

1001 19th St., North, Suite 2000
Arlington, VA 22209
P: 202.682.9110 F: 202.682.9111

TechAmerica.org
CompTIA.org

Therefore, our response will seek to summarize the input and scope of this knowledge and utilization, as delivered from our membership and the breadth of American technology industries.

Awareness

The simplest assessment of the Framework's awareness among technology organizations is to say that it varies greatly. With respect to small and medium sized companies, the record is mixed. That is why we have worked with the Department of Homeland Security's Critical Infrastructure Cyber Community Program (C3) to help educate State Tech Councils and IT companies of all sizes about the framework and its broader mission. Among those that have provided input to TechAmerica's request for feedback, awareness is very high. Many of our members played key roles in development of the Framework, and have worked closely with NIST to craft sound policy. NIST ITL bulletins and industry newsletters have served many organizations well by providing detailed progress reports and specific implementation plans.

However, it is too early in the process to assess full industry awareness, as those organizations without government relations or contracting operations do not possess the resources to fully implement and participate in the Framework.

There remains a need for greater focus on industry incentives. Congress and the Administration should cultivate an environment that spreads threat awareness, and encourages information sharing, without constructing a regulatory approach. A regulatory environment will deter participation, and promote a "bare minimum" approach that could have a catastrophic outcome for our national security.

Experience

Industry's evaluation of the Framework is ongoing, but it is too soon to assess. Many organizations have robust risk management practices in place. Many of these organizations have contributed to the development of the Framework and therefore have shared their risk management practices with NIST.

We do know that the Framework has helped some organizations review their practices to fall in line with the Framework. Many, however – and this includes international organizations – are monitoring closely the progress of the Framework, and therefore will be hesitant to implement specific changes related to the Framework until there appears to be consensus on the viability of utilization.

Roadmap for the future

TechAmerica
Powered by CompTIA

1001 19th St., North, Suite 2000
Arlington, VA 22209
P: 202.682.9110 F: 202.682.9111

TechAmerica.org
CompTIA.org

The success of the Framework and ultimately Executive Order 13636 will rely on organizational engagement, dedication by the US Government to the spirit of voluntary adoption, and an ongoing, adaptable approach to mitigating cyber threats.

Organizational engagement must primarily be conducted by NIST and partnering agencies to showcase cost/benefits to supply chain manufacturers and those industries with fewer resources than the mature, multinational organizations. The agencies that have the dollars to dedicate and the expertise, such as the Department of Homeland Security, Department of Justice, and NIST should conduct promotion of the risk management tools incorporated in the Framework. Outreach activities such as forums and seminars conducted by NIST or the Small Business Administration across the United States could prove beneficial to smaller, local organizations. Understanding the risks and the resources at hand will help smaller organizations conduct analysis and promote cyber hygiene, particularly as they seek to partner with state and local governments – whom also would benefit from this type of outreach and coordination.

Likewise, the voluntary nature of the Framework is essential to its effectiveness. In fact, it is TechAmerica's position that our nation's economy and security could be severely damaged by turning the Framework into a working regulatory approach, by either direct rule making or back door approaches such as developing Framework themes into acquisition and procurement reforms.

The market is creating a demand for network and data security – be it to protect intellectual property, personally identifiable information, or national security intelligence. The market must remain the guide for developing security standards, and many of TechAmerica members have responded to the market by addressing vulnerabilities and crafting risk management plans that have become the standards that multinational organizations rely upon.

Successful and widespread outreach, as well as dedication to the Framework's voluntary nature will prove successful if the US Government remains dedicated to recognizing and adapting to the changing nature of the threat. Industry remains concerned about federal agencies developing static measures that will become outdated before they are fully in use. American industry is driving our nation's critical infrastructure protection efforts, and the US Government should continue to look to them when developing best practices and when making decisions that impact our national security.

****

Thank you again for this opportunity to submit our perspectives on the awareness and usage of the NIST Framework for Improving Critical Infrastructure Cybersecurity. We look forward to the opportunity to continue to dialogue with NIST as we seek to make the Framework a success, and help to keep our nation's critical infrastructure secure from cyber threats. If there are any questions on this submittal, please contact me at 202.682.4422 or ehyman@comptia.org

TechAmerica
Powered by CompTIA

1001 19th St., North, Suite 2000
Arlington, VA 22209
P: 202.682.9110 F: 202.682.9111

TechAmerica.org
CompTIA.org

Sincerely,

Elizabeth Hyman
Executive Vice President of Public Advocacy
TechAmerica