Business Roundtable℠

300 New Jersey Avenue, NW
Suite 800
Washington, DC 20001

Telephone 202.872.1260
Facsimile 202.466.3509
Website brt.org

January 18, 2018

Via Electronic Submission to: cyberframework@nist.gov

Ms. Andrea Arbelaez
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 2000
Gaithersburg, MD 20899

Dear Ms. Arbelaez,

Re: Comments on Cybersecurity Framework Version 1.1 Draft 2

On behalf of the nearly 200 members of Business Roundtable, an association comprised of chief executive officers of leading U.S. companies representing all sectors of the economy, I want to thank you for the opportunity to comment on the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Framework) Version 1.1 Draft 2.

We believe that NIST's leadership in developing the voluntary and risk-based Framework has improved our nation's cybersecurity posture. The Framework provides companies of all sizes with a flexible approach to evaluate their cybersecurity posture as threats and vulnerabilities evolve.

We appreciate the opportunity to further the discussion on the Framework and offer the following comments on Version 1.1 Draft 2:

- **Business Roundtable supports NIST's formal public-private process to evolve the Framework.** We recognize that the Framework is a living document and support the transparent and collaborative process NIST has adopted to improve the Framework. We believe that this approach has produced revisions to the Framework that reflect the evolving cybersecurity ecosystem. We encourage NIST to continue to draw on expertise from the public and private sectors and consider a diverse array of threats, vulnerabilities, and risks as the Framework expands into new areas.

- **Business Roundtable encourages NIST to promote the Framework as a model for harmonizing cybersecurity requirements across federal and state regulatory bodies.** We urge NIST to educate U.S. government agencies and state and local governments on the benefits of using a common flexible, risk-based approach for cybersecurity. Our companies are concerned that agencies do not make consistent use of the Framework in shaping the regulatory environment for cybersecurity. Reconciling disparate and sometimes conflicting requirements diverts corporate resources toward legal compliance activities rather than risk-based cybersecurity measures. We support a consistent government-wide approach to cybersecurity risk management that aligns with the Framework.

In addition, state proposals to regulate cybersecurity continue to grow, creating a patchwork of regulations across states. We recommend that NIST work with state governments to emphasize the importance of risk-based approaches to cybersecurity and to encourage the use of the Framework.

- **Business Roundtable encourages NIST to continue to explore cybersecurity measurement concepts with stakeholders.** We support the revised section on measurement that is focused on the value of self-assessments of cybersecurity risk. Cybersecurity risk assessments benefit many internal stakeholders by facilitating decision making and linking decisions to business objectives. However, we are concerned about third parties using metrics and measurement tools to assess cybersecurity performance given the lack of universal measurement approaches and a standard taxonomy for basic terms like "metrics" and "measurement." Most approaches for measuring cybersecurity performance are underdeveloped and require further maturation before they can be incorporated into an organization's overall risk management framework. Many stakeholders also lack data to generate quantifiable risk approaches.

  In addition, we believe that companies should have complete control over the use and disclosure of any measurement data they create, subject to existing laws, regulations, or contractual agreements. The Framework should clarify that outside parties should not be given access to measurement data without company authorization.

  Business Roundtable encourages NIST to lead a process—in collaboration with industry, academia, and government—to resolve gaps associated with cybersecurity performance measurement. This process should prioritize input from experts in actuarial and data sciences, risk quantification, and insurance underwriting. In addition, Business Roundtable strongly encourages NIST to explore new data sources that both public and private sectors may leverage to create meaningful metrics, increase organizational understanding of cybersecurity risk, and ultimately develop a strong performance management culture for cybersecurity. Finally, if the Framework is to include a section on risk quantification and metrics, we strongly encourage NIST to work closely with all stakeholders to review additional risk quantification challenges, including the lack of a standard taxonomy or vernacular on cybersecurity measurement topics, and to address such challenges in future iterations of the Framework.

- **Business Roundtable appreciates the Framework's increased focus on supply chain risks.** Our members, as global companies, fully appreciate the importance of managing IT supply chain risks. Security approaches for managing supply chain risks vary widely across organizations and sectors. NIST should ensure that supply chain risk management (SCRM) guidance is risk-based, technology neutral, and adaptable for companies to apply practices that are best suited to their business. In addition, NIST should encourage use of the Framework across the supply chain and use the Framework to align development of various evolving global cybersecurity directives and legislative initiatives.

- **Business Roundtable supports vulnerability disclosure processes but encourages NIST to prioritize further dialogue with the stakeholder community on this complex topic.** We support NIST's incorporation of a new subcategory focused on standing up a vulnerability disclosure process to receive, analyze, and respond to vulnerabilities, and we appreciate NIST's work to draw attention to this important issue. However, we believe additional dialogue is needed among stakeholders to understand complexities associated with vulnerability disclosure, including how to staff, finance, and manage such programs. We encourage NIST to prioritize additional engagement with industry, security researchers, and the government to address such complexities in its Roadmap activities.

- **Business Roundtable encourages NIST to continue promoting adoption of the Framework by all sectors.** We support NIST's clarification that the Framework can be used by organizations "in any sector or community" regardless of their size, focus, or sophistication. NIST should continue to identify ways to incentivize greater adoption of the Framework by all types of organizations.

- **Business Roundtable supports the development of additional sector-specific cybersecurity profiles and use cases.** We applaud the creation of sector-specific cybersecurity profiles by the financial services and manufacturing sectors. Sector-specific profiles make the Framework more useful by highlighting the unique needs of individual sectors while recognizing the importance of a common framework. In addition, we support the creation of case studies and use cases that provide companies with greater detail on implementation. NIST should work with and encourage other sectors and communities to develop and publish additional profiles and use cases.

- **Business Roundtable appreciates that NIST elaborated on the Framework Implementation Tiers.** The additions NIST made to the Implementation Tiers make it easier to understand how the tiers are intended to be used and the relationship between the Tiers and an organization's Target Profile. In addition, we support the refinement of the Implementation Tier criteria, including the simplification of language related to SCRM.

- **Business Roundtable encourages NIST to tailor Framework resources to the needs of small- and medium-sized businesses.** Cybersecurity threats and vulnerabilities affect businesses of all sizes. We encourage NIST to continue developing the Framework, and complementary resources, to ensure that our nation's small- and medium-sized business community can be a full partner in cybersecurity risk management.

- **Business Roundtable urges NIST to continue engaging with international stakeholders.** We support NIST's efforts to promote the Framework with other countries and international standards bodies. The adoption of interoperable international cybersecurity standards is essential to the growth and development of the digital economy. Complementary standards across jurisdictions provide global companies with a common taxonomy for assessing risks, thereby improving the efficiency across jurisdictions and throughout global supply chains. The standards, guidelines, and practices generated by the Framework are scalable across borders and reflect global risks and threats. We support NIST's continued international outreach to encourage foreign governments and international standards organizations to leverage the Framework in a manner that enables harmonization and complementary standards, guidelines, and best practices.

  In addition, we applaud the U.S. government for including language that promotes the use of voluntary cyber risk management frameworks in the North American Free Trade Agreement negotiations, and we urge the U.S. government to advocate for the inclusion of this language in all future trade agreements.

In summary, we believe that a flexible, technology-neutral, and risk-based Framework developed through active collaboration with industry is the most effective way to strengthen cybersecurity for all sectors of the U.S. economy. We applaud NIST for its work in this space.

Business Roundtable promotes use of the Framework with our member companies and believes the Framework provides a solid baseline for cybersecurity risk management practices. Many of our member companies leverage the Framework in various ways. We believe that updating the Framework is important to address evolving threats and trends. The proposed changes will result in greater awareness of emerging cybersecurity challenges within the corporate community at home and will support the continued proliferation of the Framework across key business communities abroad.

Business Roundtable appreciates NIST's consideration of our comments and looks forward to continued collaboration to shape the programs that the private sector uses to manage cybersecurity risks.

Sincerely,

Julie Sweet
Chief Executive Officer - North America
Accenture
Chair, Technology, Internet and Innovation Committee
Business Roundtable