From: **Gasster, Liz**
Date: Mon, Apr 10, 2017 at 3:39 PM
Subject: Business Roundtable: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Please see the attached comments on the draft update of the framework for improving critical infrastructure cybersecurity on behalf of Julie Sweet, Chief Executive Officer – North America, Accenture and Chair of the Technology, Internet and Innovation Committee at Business Roundtable.

Business Roundtable
300 New Jersey Avenue, NW | Suite 800 | Washington, DC 20001
Main Phone: (202) 872-1260 | Fax: (202) 466-3509

www.brt.org
www.brt.org/blog

[Attachment Copied Below]

April 10, 2017

Mr. Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Mr. Games:

Re: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

On behalf of the close to 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.

We believe that NIST's leadership in developing the voluntary and risk-based framework has improved our nation's cybersecurity posture. Unlike prescriptive, one-size-fits-all regulations, the Framework provides the management of all sizes of organizations with a flexible approach to evaluate their cybersecurity posture as threats and vulnerabilities evolve.

We appreciate the opportunity to provide the following comments on Framework Version 1.1, and we offer the following observations:

- **Business Roundtable encourages NIST to continue to perform outreach internationally with the Framework:** The standards, guidelines and practices generated by the Framework are scalable across borders and reflect global risks and threats. Complementary standards across jurisdictions will enable global companies to have a common and shared taxonomy for assessing risks, thereby improving the efficiency across jurisdictions and throughout global supply chains. Despite the benefits of the Framework, there is a growing potential for conflicting and redundant cybersecurity standards, guidelines and practices that may potentially shift an organization's focus from risk management to legal compliance, potentially undermining better security choices. Therefore, we support NIST's continued international outreach to encourage governing bodies around the world to leverage the Framework in a manner that enables harmonization and complementary standards, guidelines and practices.

- **Business Roundtable supports the increased emphasis on senior leadership's role in governance and risk assessments:** As a CEO-led organization, we are especially focused on enhancing senior corporate officers' and boards of directors' understanding of their organization's security and resilience posture. Such capabilities are essential to making complex security judgments and risk-based investment decisions within a firm's governance model. We commend NIST for considering the important role of senior executives, whether experts in cybersecurity or otherwise, to assess and manage risks as part of an overall business strategy. Framework Version 1.1 appropriately emphasizes

the importance of expanding senior management's understanding of cybersecurity risks. To further enable senior management's oversight of risk-based controls, we recommend NIST develop a process for organizations to determine the key areas of their inherent risks that align with the categories in the Framework. This would provide additional guidance to senior executives in making these cybersecurity investment decisions for their organizations in the context of an overarching risk management strategy.

- **Business Roundtable appreciates NIST's recognition of growing threats against the private sector and encourages additional focus on risks stemming from interdependencies with third parties:** We support the continued focus on cybersecurity threats against the private sector. Our nation's businesses are increasingly on the front lines of sophisticated cyber threats that attempt to steal our intellectual property and undermine confidence in our economy. Our national economic security depends on U.S. enterprises' network defenses to safeguard systems and data and to provide secure and resilient services. However, our businesses also depend on global supply chains and third parties to provide our products and services. As a result, our risk assessments need to account for evaluating and measuring risks that come from third parties. Therefore, we support NIST's expansion of the focus of the Framework to include third-party relationship risk management.

- **Business Roundtable supports Framework Version 1.1 guidance for small- and medium-sized businesses:** We recognize the importance of accessible and practical risk management frameworks and related support for smaller businesses . Cybersecurity threats and vulnerabilities affect businesses of all sizes. We encourage NIST to continue developing the Framework and complementary guidance and resources to ensure that our small business community has appropriate guidance and resources to be a full partner in cybersecurity risk management. We also encourage NIST to support legislative and executive branch policies that would support its capacity to engage more directly with the small business community.

- **Business Roundtable supports a formal process to evolve the Framework:** We recognize that Framework Version 1.1 is a living document and support NIST's use of a formal collaborative process to drive Framework evolution, including coordinating with industry. There are few industry-driven and government-led processes to examine complex cybersecurity challenges. We encourage NIST to continue to draw on expertise from the public and private sectors and consider a diverse array of threats, vulnerabilities, risks and other key inputs as the Framework is updated.

In sum, 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.

Business Roundtable appreciates NIST's consideration of our comments and looks forward to continued collaboration to shape the cybersecurity 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