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

19 January 2018

Dear Ms. Arbelaez,

PwC is pleased to provide feedback on Draft 2 of NIST's Cybersecurity Framework Version 1.1 and the accompanying Roadmap. We believe the good principles outlined in the Framework have the potential to help countless organizations make basic cyber hygiene part of their muscle memory, an essential foundational step in the development of robust cyber risk management that is more proactive than reactive.

Since NIST issued the initial Framework in 2014, PwC has advised clients on the many potential benefits of adopting the Framework.[1] The relevance of the Framework has continued to grow as organizations from a wide array of sectors put it into action. For example, in PwC's 2018 Global State of Information Security® Survey (GSISS), respondents from healthcare payer and provider organizations, as well as oil and gas companies, say the NIST Cybersecurity Framework is the most commonly adopted set information security standards in their respective industries. Further, many financial institution clients embrace benchmarking of their cyber risk management programs against the NIST Cybersecurity Framework. We applaud NIST for its continuing engagement with the private sector to further strengthen the Framework. Companies need powerful tools to manage powerful risks.

Many companies are not as prepared as possible to deal with cyberattacks. In the 2018 GSISS, 44% of the 9,500 executives from all industries surveyed say they lack an overall information security strategy.[2] In addition, 48% say they do not have an employee security awareness training program and 54% say they do not have an incident-response process. Consumers are understandably worried. In our recent US Consumer Intelligence Series survey, more than two-thirds of 2,000 US consumers surveyed believe that businesses are highly vulnerable to cyber threats.[3] Only 25% of the consumers we surveyed say they believe most companies handle their sensitive personal data responsibly.

Relative to the initial version, Draft 2 of NIST's Cybersecurity Framework Version 1.1 makes a number of positive changes, including language clarifying the Framework's applicability to supply chain risk management and the internet of things (IoT) and language on using the Framework for self assessment.

[1] PwC, Why you should adopt the NIST Cybersecurity Framework, May 2014
[2] PwC, Strengthening digital society against cyber shocks, October 2017
[3] PwC, Consumer Intelligence Series: Protect.me, November 2017

One general recommendation to NIST for further strengthening the Framework is to make language as proactive as possible. Organizations that bring a proactive mindset to the challenges of managing end-to-end cyber and privacy risks and building resilience are more likely to sustain operations when faced with disruptive threats and thrive in the digital economy. Taking the initiative to manage cyber and privacy risks before a crisis erupts is also what today's consumers expect from business leaders. In our recent US Consumer Intelligence Series survey, 92% of consumers surveyed say companies must be proactive about data protection and not wait for the government to enact regulation.

We also recommend the following specific changes to the Framework:

- In the Framework Introduction, line 180, add the following at the end of the paragraph: "Organizations should also consider what interdependencies might exist between critical and non-critical assets and how to manage related risks."
- In Methodology to Protect Privacy and Civil Liberties, line 750, expand the first sentence to read as follows: "Privacy and cybersecurity have a strong connection and are increasingly intertwined."
- In Methodology to Protect Privacy and Civil Liberties, line 764, where it states "To address privacy implications, organizations may consider how their cybersecurity program might incorporate privacy principles…" replace "may" with "should"

In addition, we have a few comments about specific sections of the Roadmap:

- **Section 4.1:** We agree with NIST's view that market-based efforts to develop confidence mechanisms related to the Framework have the potential to help organizations determine the sufficiency and efficacy of organizational cybersecurity risk management.
- **Section 4.6:** We welcome NIST's interest in collaborating with industry on discussions about corporate and board governance and enterprise risk management and look forward to participating in the dialogue.
    - As noted in our recent GSISS paper, *Strengthening digital society against cyber shocks*, "C-suites must lead the charge—and boards must be engaged."[4]
    - Regarding ERM, we believe the pairing of the NIST Cybersecurity Framework with the COSO ERM Framework, for example, could provide synergies in cyber risk management efforts.
    - The elevation of cyber risk as a risk category distinct even from operational risk and the translation of cyber risk data into actionable risk intelligence for executive management and boards of directors should in our view be an ERM imperative.
- **Section 4.9:** We support NIST's plans to continue discussion on measuring cybersecurity and the linkage of cybersecurity to business objectives and decisions. We agree with NIST that establishing stronger connections between these issues could create greater efficiency, richer dialogue and more useful answers to questions about cost effectiveness and return on investment.

[4] PwC, Strengthening digital society against cyber shocks, October 2017

- **Section 4.10:** We believe NIST's continuing focus on privacy engineering is good news for technology developers, privacy professionals, and consumers. Efforts to boost dialogue between the technology and privacy communities could help foster the development of more devices designed with security and privacy in mind.

PwC's mission is to build trust and solve our clients' most important problems. PwC's Cybersecurity and Privacy practice, led by Sean Joyce, offers its perspective on the NIST Cybersecurity Framework and Roadmap in that spirit and looks forward to participating in further dialogue.