National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW
Room 4725
Attn: Cybersecurity RFC 2015
Washington, DC 20230

Dear Mr. Friedman,

We respectfully write in response to the National Telecommunications and Information Administration's ("NTIA") request for comments regarding Stakeholder Engagement on Cybersecurity in the Digital Ecosystem ("Cybersecurity Engagement").

ABOUT INTUIT

Intuit was founded in Silicon Valley more than 30 years ago, and is dedicated to using technology innovation to solve important financial management problems for consumers and small business. Our mission is to improve our customers' financial lives so profoundly they can't imagine going back to the old way. Our customers include micro, small and medium-sized businesses, consumers, and accounting professionals. We help them manage their finances, pay bills and employees, prepare and file their income taxes. Our innovative products and services simplify the lives of more than 50 million people, helping them save and make money.

INTUIT COMMENTS

Intuit cares deeply about security, especially in the 21st century digital economy; we have seen firsthand the consumer harm that occurs when data such as personal identity information is misappropriated in the global marketplace by bad actors and subsequently used to facilitate fraud in another context. We applaud NTIA for gathering information and convening relevant stakeholders in public-private partnership to understand potential risks to businesses of all sizes and their customers.

Given the extraordinary breadth of the topic and the myriad angles that stakeholders might examine, Intuit urges NTIA to narrow the focus of its efforts to optimize the effectiveness of the effort and subsequent impact. For NTIA's efforts to positively influence policy development, stakeholders should focus on assessing the ever-evolving digital threat landscape. Broader efforts risk getting bogged down by widely conflicting agendas of stakeholders. Cybersecurity is too important to consumers and businesses to let this opportunity for dialogue between and amongst stakeholders slip by without making progress at understanding the actual nature of the emerging threats faced by government, business and consumers.

An assessment of risk is also likely to produce the most beneficial outcome to help guide responses to evolving risks. Information sharing, achieved through stakeholder dialogue, could prove highly valuable in identifying gaps in the current security policy framework, as well as trends and emerging challenges. That could lead to the development of a set of outcomes-based best practices that entities could adopt to protect customer data from vulnerabilities that lead to identity theft and account takeover.

One area within the Request for Comments deserving attention is that of Web Security and Consumer Trust. Intuit urges a focus on the challenge of authenticating customers in cyberspace. While this is a high value subject to tackle, we also encourage NTIA to be cognizant of and not replicate the work of similar federal bodies. In particular, NTIA should not recreate the work of the National Strategy for Trusted Identities in Cyberspace ("NSTIC"), which has convened for the last 4 years to develop a set of potential technical protocols to facilitate secure authentication in cyber-space. By contrast, we see the value of the Cybersecurity Engagement as an opportunity to review the current state of actual cybersecurity threats and determine whether there are gaps in the policy landscape that could be closed by addressing them via a multi-stakeholder-driven code of conduct and best practices.

Finally, if the Cybersecurity Engagement leads to adoption of consensus recommendations, we believe they must be technology neutral, neither favoring nor condemning any particular technology, security protocol or proprietary solution. Businesses and governments are best positioned to understand their own risk profile, and are continually adapting technologies to counter and stay one step ahead of bad actors. Any efforts to direct or limit the flexibility of responses is likely to produce more harm and vulnerability than benefit. Surely, not every security protocol will be appropriate for every setting or for every type of data.

Intuit looks forward to participating in the Cybersecurity Engagement. This is an important initiative that needs to move forward, with a sound framework that will optimize the effectiveness and impact of the effort.

We appreciate the opportunity to offer comments. Thank you for your time and attention to this critically important issue.

Bernard F. McKay
Chief Public Policy Officer,
Vice President for Corporate Affairs
Intuit, Inc.