January 18, 2017

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

Via e-mail to: cyberframework@nist.gov

Dear Mr. Games:

Thank you for allowing Amazon Web Services to comment on the "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2" (herein "CSF"). We are encouraged to see updates to Draft 2 that will broaden the use of the CSF and continue to reinforce its organizational-, sector-, and country-agnostic approach to cybersecurity risk management and resilience. We offer the following comments on Draft 2 and appreciate NIST taking the below into consideration.

1) **Section 2.1 Framework Core**- **Modify the name of the "detect" function to "monitor."** We believe that "monitor" better suits the name of this function. Detect has the connotation of potentially being a one-time event, where monitor is ongoing. Redefining the function will also serve as a reminder that the functions themselves should all be monitored and improved as necessary. All of the functions are integrated into a feedback loop as part of continuous monitoring and improvement, much in the same way the aviation industry not only reacts and responds to accidents but actively learns from them and implements improvements in policies, procedures, design, operations, etc.

2) **Section 2.4 – Coordination of Framework Implementation.** We recommend an introductory paragraph to describe the internal organizational "coordination" efforts necessary to ensure proper implementation of the CSF. All too often, the views of one part of an organization will outweigh another, resulting in unilateral decision making that does not reflect a comprehensive, organizational view. Given the CSF's flexibility to be used as a common best practices framework ranging from executive leadership to technical systems administrators (and the roles that fall in between that spectrum), greater focus on coordinated implementation would support the success of its integration. A flow down from senior leadership and business is essential for guidance and direction, and a flow up from implementation and operations is equally essential to help identify any technical limitations or enablers.

3) **Section 3.0 How to Use the Framework (line 570)-** We recommend that an "architecture" step be added prior to design. The architecture step will allow a preliminary investigation into the program, schedule, and budget necessary to continue with a CSF that is appropriate

for the organization. If there is no need to construct a particular cybersecurity defense then designing one may be wasteful.

4) **Section 3.3 Communicating Cybersecurity Requirements with Stakeholders**. In this section the CSF provides 5 different examples to illustrate the importance of using "a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure products and services." Two of the examples explicitly call out external resources. We believe that there are also internal stakeholders that may be part of the supply chain that will play a critical role in the delivery of infrastructure and services. As an example, a government agency may have employees that specialize in physical security. These employees could be assigned to protect an on premise data center, bypassing the need to use external resources. An example of an internal stakeholder should be included to illustrate that interdependent stakeholders can be both internal and external.
5) **Section 3.4 Buying Decisions**. Similar to the comment we provide in Section 3.3, some buying decisions may be internal and not rely on an external provider. These internal suppliers can be internal and the decision to "buy" might also be a "decision to consume" internal resources. As an example, a power company can choose to use their own power-plants to supply electricity to power on premise security components or "buy" power from the grid.
6) **ID.SC-3**: We would like you to consider adding the highlighted phrase at the end of this section: *Suppliers and third-party partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan* ***commensurate with the type of service offered****.* When using cloud technology there is a shared responsibility between both the Cloud Service Provider (CSP) and consumer. For example, with Infrastructure as a Service (IaaS) cloud technology, the CSP manages security *of the cloud*, and security *in the cloud* is the responsibility of the customer.

Finally, AWS would like to take this opportunity to thank NIST for seeking out comments from its private sector stakeholders to ensure a safe, secure, and resilient cloud computing environment for the world. We look forward to working with NIST to promote a universally-adaptive approach to effective cybersecurity risk management for organizations of any size, in any sector, and from any geography.

Sincerely,

John Britton
Sr. Strategist
Amazon Web Services