January 19, 2017

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

Re: Symantec Response to Version 1.1, Draft 2 Update of the Framework for Improving Critical Infrastructure Cybersecurity

Symantec is pleased to submit the following comments on Draft 2 of Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity (CSF). Symantec continues to incorporate the CSF into multiple aspects of our business, both internal and external. We remain strong advocates of the CSF and have dedicated resources to educate organizations and individuals across multiple industry verticals and promote the adoption of the Framework. We have conducted numerous Webinars across multiple industry verticals, including a seven-part series focused on the value of the CSF in Healthcare (NIST co-presented Part 3 with us.) Often the most informative portions of our webinars are the Q&A and the suggestions below reflect feedback we have received.

Our submission is divided in to two sections. Section one is our overall response to Draft 2, while section two provides suggestions for additional changes for NISTs consideration.

Additional Changes to Consider

1. The Benefit of the CSF in a "Regulated" Environment

We are often asked variations of the same question: "I already use/am regulated to use (PCI, HIPAA, SANS 20, FISMA, etc.). Why should I also use the CSF?" This question is often asked in the context of justifying the effort to adopt the CSF or the cost of the resources and funds required to do so. It would be helpful if the next version of the CSF included a section addressing this question head on. This section could include the following points, which we have refined over numerous discussions with customers.

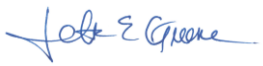
- The evidence being collected for other control families can be reused (via mapping) for the CSF subcategories. The effort to implement SANS, for example, are not wasted when using CSF.
- The CSF allows a user to view existing data in a new way. For example, take the question of how mature is an organization' ability to manage assets?
    - FISMA requires looking at 11 Controls across 8 Control Families.
    - The CSF has this in one Category, broken down into Six Subcategories
    - Viewing this information grouped together facilitates deeper analysis and may lead to different operational decisions.

- Other standards/frameworks may be limited to certain threat vectors (PCI, HIPAA) leaving many unaddressed threats, while the CSF takes a holistic viewpoint.
- The CSF can be used to assess against specific threat vectors. For example, if ransomware is a concern, the CSF can be used to isolate particular subcategories associated with addressing this threat and assessing against them tactically.

2. Our final suggestion is a potential Roadmap Item - development of a matrix that aligns subcategories to threat vectors (similar to Informative References) to allow for tactical assessments. The matrix would need to be a "living document" periodically updated as new Threats emerge, but could be a powerful tool to help organizations find additional ways to utilize the CSF.

Thank you for the opportunity to provide our response to the proposed update to the CSF. We would gladly make ourselves available should you wish to discuss our comments in more detail.

Sincerely,



Jeff Greene
Senior Director, Global Government Affairs
& Cybersecurity Policy
Symantec Corporation