From: **Jeff Greene**
Date: Mon, Apr 10, 2017 at 1:20 PM
Subject: Symantec comments on Draft CSF version 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

To whom it may concern –

Attached are Symantec's comments to the draft Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Please let us know if you have any questions.

Jeff Greene
Senior Director, Global Government Affairs & Policy

Symantec Corporation
www.symantec.com

700 13th Street, NW
Suite 1150
Washington, DC 20005

[Attachment Copied Below]

April 10, 2017

VIA EMAIL
cyberframework@nist.gov

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

Re: Symantec Response to Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

Symantec is pleased to submit the following comments on the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity (CSF). We have incorporated the CSF into multiple aspects of our business; we use it internally to assess, improve and communicate results of our cybersecurity posture, and we have also integrated it into our sales, marketing and product development to assist clients in their use of the tool. Additionally, we have invested heavily in educating the community on how to use the CSF, including webinars for broad audiences as well as for specific industry verticals. These webinars are available online for the public to view. We look forward to participating in the CSF update process.

Our submission is divided in to two sections. Section one provides comments on the proposed changes, while section two provides suggestions for additional changes for NISTs consideration.

Section One: Comments on Proposed Changes

1. Strengthening authentication & identity management in the Framework Core:

We were pleased to see movement on the Authentication Roadmap Item, but were surprised to see that a critical security control such as Multifactor Authentication (MFA) was left out. MFA is a proven technology that addresses a major threat vector and at minimum should be presented as a specific option for CSF consumers. We recommend including a specific control to address MFA in the PR.AC section of the Framework.

2. Guidance for acquisition and supply chain risk management (SCRM):

We support the specific focus on supply chain risk management (SCRM). SCRM is an often overlooked threat vector that needs specific attention in today's cyber threat environment. Using the acquisition process to enforce SCRM could be effective as long as it doesn't become a "check the box" exercise and is done in a way that recognizes the complexities of the global supply chain.

3. Methodology for measurement and generating metrics:

We support the addition of a section on "measurements and metrics" to the CSF. Although metrics can be misused as an oversimplified "checklist" approach, if applied correctly they are an invaluable tool to set business goals, define a project and milestones, and align an organization behind a security effort.

Therefore, we suggest NIST identify an industry best practice or develop measurement and metrics best practices that provide the ability to define and manage a security project without being too prescriptive.

4. Clarity on Implementation Tiers and their relationship to Profiles:

We support the additional clarity concerning Tiers in the CSF process. In our experience, it is one of the most misunderstood aspects of the CSF. Organizations apply the Tiers in varying ways. Some apply it to the organization as a whole, while others have modified Figure 1: Framework Core Structure, to add the Tiers at Function, Category or Subcategory level and made it work for them. There may be value in adding a modified Figure 1 to illustrate the creative ways to implement Tiers in the CSF process.

Section Two: Additional Changes to Consider

"Step 4: Conduct a Risk Assessment":

We understand the Framework was designed so that a user selects a risk assessment process to use in Step 4. However, the Framework does not provide guidance on how to conduct the required risk assessment. Absent such guidance, less mature organizations could choose not to use the Framework – or if they do use it, they may not take full advantage of it. We would suggest development of a section similar to Section 2.2 "Managing Your Risks" of the NISTIR 7621 Rev. 1 "Small Business Information Security: The Fundamentals. Alternatively, the CSF could reference NIST Special Publication 800-30 Rev. 1, *Guide for Conducting Risk Assessments,* as a starting point.

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,

Jeffrey E. Greene
Senior Director
Global Government Affairs and Policy