December 13, 2013

VIA EMAIL
csfcomments@nist.gov

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Re: Request for Comments on the Preliminary Cybersecurity Framework
(Docket No. 130909789–3789–01)

Dear Mr. Sedgewick:

Symantec appreciates the opportunity to provide comments on the preliminary version of the Cybersecurity Framework ("Framework"). As a global leader in providing security, storage, and systems management solutions, Symantec is committed to assuring the security, availability, and integrity of our customers' information. Today, we protect more people and businesses from more online threats than anyone in the world. We maintain eleven Security Response Centers globally and utilize over 69 million attack sensors that record thousands of events per second. Improving the cybersecurity of our nation's critical infrastructure is essential to securing the Nation's national and economic security, and we are pleased to be able to assist the National Institute of Standards and Technology (NIST) in developing the Framework.

As an initial matter, we want to express our appreciation for the open and inclusive process that NIST employed to develop the preliminary Framework. NIST's outreach to the private sector was extensive, and the Framework workshops were well-planned and informative. Most importantly, NIST was responsive to the comments submitted by Symantec and the many other organizations that participated in the process. Indeed, the preliminary Framework reflects many of these, and was improved by the feedback NIST obtained during the development of the draft.

The preliminary Framework is a strong document. It provides a structure that can be used by organizations of all sizes, whether they have a sophisticated cybersecurity program in place or are just beginning to assess their needs. A large company that has a mature cybersecurity program can use the Framework as a tool to examine its assumptions and procedures. Conversely, a small organization that is just beginning to address its cybersecurity risks can use the Framework to assess its needs and to develop a program. The Framework also provides a simple, common set of terms that are useful when discussing cybersecurity matters with corporate leaders and executives; in fact, we have already mapped the five preliminary Framework Core Functions to our internal security program and briefed it to our Board of Directors.

We were also pleased to see that the preliminary Framework is neutral in three key areas. First, it is technology neutral, as it does not prescribe any specific approach or technology. Second, it does not favor any individual standard or practice that could be used to achieve a given security goal, instead encouraging organizations to determine how best to meet their cybersecurity needs. Finally, it is geographically neutral, as it neither creates a "US-specific" security standard nor promotes US-based practices or standards.

This neutrality gives the preliminary Framework the flexibility it will need if it is to be widely adopted by US-based global companies and if it is to have continued utility in the future. The cyber threat landscape is continually evolving, and the Framework will not endure if it does not evolve along with it. As currently structured, the preliminary Framework encourages organizations to implement the type of flexible security model that can change as technology and threats shift.

Areas for Improvement

There remain several areas where the preliminary Framework can be improved. We have provided specific edits and suggestions in the attached spreadsheet, and below offer additional suggestions for improving the preliminary Framework's utility and increasing the likelihood that an organization will adopt it.

- We recommend the addition of a concise and prominent list of the Framework's core principles early in the document. Currently these are spread throughout the document, and it would be useful to compile them so that there is a single statement of what the Framework is – and more importantly – *is not*. Some of these principles could include:
    - "The Framework Core is not a checklist of activities to perform"[1];
    - "The Informative References presented in the Framework Core are not exhaustive but are example sets, and organizations are free to implement other standards"[2]; and
    - "The Framework is designed to complement existing business and cybersecurity operations."[3]

  Further, NIST representatives stated at the workshops that few organizations will need to strive for "Tier 4: Adaptive" in many of the core functions, and in fact few if any will need to be Tier 4 in all of the functions. NIST acknowledged that reaching and maintaining Tier 4 would be costly (particularly for small and medium businesses) and will often make no sense given a company's risk profile. The preliminary Framework itself does not reflect this, however. The core principles should include a statement that in most use cases lower tiers are not only acceptable, but are in fact appropriate. It is important that the Framework not be misinterpreted as a call for all organizations to seek the highest level of security, irrespective of need or cost.
- We believe there should be a communications aspect to the "DETECT" function. Many times organizations detect incidents because of communications received from partners or third party sources. As such, there need to be reliable processes in place to ingest and evaluate shared information to improve detection. Moreover, mature organizations should actively seek sources of new threat and vulnerability information.
- It is implicit throughout the preliminary Framework that good cybersecurity requires continuous assessment and improvement, and that the plan that an organization makes when it begins the Framework process will need to be reviewed and often updated during implementation. Nevertheless, it would be beneficial for NIST to state this clearly and concisely.
- The preliminary Framework rightly recognizes that many organizations that consider adopting it will have in place existing cybersecurity programs and risk management processes. However,

[1] *See* Preliminary Framework, p.4. http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf
[2] *See id.* at 6.
[3] *See id.* at 11.

the Framework never answers the question of *why* an organization that has such a program or process should look to the Framework rather than continuing its existing effort.

- Many organizations that look to adopt the Framework will be subject to existing regulatory requirements or will be using well-known security standards or protocols. It would be useful if the Framework included a discussion and an illustrative example of how NIST envisions the Framework integrating with existing requirements. Examples include the Health Insurance Portability and Accountability Act (HIPAA) data security standards and the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards.
- Many organizations that adopt the Framework have numerous components within them, and very often each will have different security requirements and threat profiles. As such, adoption will mean different things in different parts of the organization. For instance, the component of an energy company that controls generation and distribution of electricity will have a different security profile than the component that maintains a public facing website. Yet the Framework suggests that this company should have one profile that is set at the organization level.[4] The Framework should expressly recognize that it can – and should – be implemented differently within one organization.
- The preliminary Framework identifies authentication as an "Area for Improvement" and suggests that innovation is needed in this area. The body of the Framework, however, makes no mention of authentication as an element of any of the core functions, categories, or subcategories. NIST, in consultation with industry, should identify how authentication (the concept, not a specific solution) fits into the categories and subcategories, both because it is an essential element of a comprehensive security approach, and because increased prominence could help spur the innovation NIST seeks. As the White House noted in a recent blog post, secure identity solutions are essential to the security of critical infrastructure.[5]

Symantec thanks you for the opportunity to provide this input, and to assist in the development of the Framework. We have appreciated working with you throughout this process, and please do not hesitate to contact us if you need additional information or if we can be of further assistance.

Sincerely,

Cheri F. McGuire
Vice President
Global Government Affairs & Cybersecurity Policy

Enclosure

[4] *See id.* at 2.
[5] *See* http://www.whitehouse.gov/blog/2013/12/09/trusted-identities-secure-critical-infrastructure