February 23, 2016

VIA EMAIL
cyberframework@nist.gov

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: Views on the Framework for Improving Critical Infrastructure Cybersecurity
[Docket No. 151103999-5999-01]

To Whom It May Concern:

Symantec appreciates the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on the Framework to Improve Critical Infrastructure Cybersecurity (Framework). Symantec protects much of the world's information, and is the largest security software company in the world with over 33 years of experience developing Internet security technology. We worked closely with NIST during the development of the Framework, and have used it both internally and with our customers. As a result, we are well positioned to provide insights into where the Framework has worked well and where it can be improved, and attach our responses to the RFI in the requested format.

Improving the cybersecurity of our nation's critical infrastructure is essential to securing our national and economic security, and we applaud NIST's continuing efforts to work collaboratively with industry to do so. Symantec thanks you for the opportunity to provide this input, and to assist in the continued development of the Framework. 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

Attachment (RFI Response Template)

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Symantec is the largest security software company in the world, with 33 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Symantec worked closely with NIST during the development of the CSF and is eager to continue this partnership. We have experience with the CSF from two perspectives - as a consumer of the document who has used it to assess and improve our own security, and as a facilitator who has assisted our customers in understanding and using it.	
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	We are a user, a subject matter expert, and an organization that has assisted others in using the CSF. This reply was coordinated with CSF users and subject matter experts within Symantec, some of whom participated in developing the CSF.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Symantec considers the CSF when developing internal security policies and practices. The CSF is one of several frameworks that we use to evaluate our internal security control posture. Additionally, we map our products to the CSF and utilize this mapping to discuss security posture maturity with clients. We have also used the CSF to frame discussions of our own security posture and preparations with our Board of Directors.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	The Core and Profile portions provide appropriate context and we use them as sources for our internal audit activities. In addition, we found it very helpful to map our security activities to the Implementation Tiers.	
5	What portions of the Framework are most useful?	The Implementation Tiers and the Roadmap.	
6	What portions of the Framework are least useful?	Some of our clients have reported to us that they find the Tiers difficult to use, and that they have found that their profile can pre-determine the tier levels. We have also heard some customers say that the Respond & Recover elements appear to receive less emphasis than the other three, and point to the scarcity of controls in this area.	

#	Question Text	Response Text	References
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	The CSF, as a methodology for the creation of an information security function within an organization is useful. However, lack of third party certification and US government agency adoption as a security standard has hindered its full acceptance within the marketplace and in some cases has limited its value in defining and driving enhanced security. It also competes with many other industry, national, and international standards for relevancy in driving decision making and framing discussions. With that said, it does stand on its own merits as a logical guidepost for those looking to enhance security as resources permit.	
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	We do not have metrics specific to our use of the CSF. It is one of several standards and regulations that drive security considerations in what would otherwise be a purely business environment, and the implementation of security controls/solutions harden our environment and reduce risk. However, the CSF has been an effective tool in assessing our security posture and informs the consideration of new measures. In that way, it has reduced the probability of a compromise and lessened the impact of one that might occur. Measuring this reduction more broadly would require comparative data across industries involving CSF adoption maturity and breach statistics over time.	
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	The CSF can be an effective regulatory tool if regulators work together to identify overlapping mandates and determine where CSF use could assist in satisfying that requirement. The starting point should be understanding what regulatory mandates exist in the cyber realm and determining any that are identical or substantially similar. From there regulators can work together to develop a single method for compliance that satisfies multiple obligations. Additionally, new cyber regulations or tools should consider whether the target sectors or industries are already using the CSF. For example, after the Federal Financial Institutions Examination Council published its Cybersecurity Assessment Tool, some covered entities reported that using it would necessitate re-education of Board Members and other executives who had already invested time learning about the CSF. Early coordination by other agencies with NIST, and consideration of how and where the CSF is actually being used, can help avoid this in future.	

#	Question Text	Response Text	References
10	Should the Framework be updated? Why or why not?	Symantec believes that it is an appropriate time to convene stakeholders to review the CSF and refresh or update it as needed. However, given the relative newness of the CSF, NIST should resist calls for a wholesale rewriting of the core document.	
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.	The "Steps for Establishing or Improving a Cybersecurity Program" in Section 3.2 can be a source of confusion, particularly for organizations new to cybersecurity. This confusion arises from the fact that steps 1, 2, 4, and 7 are not covered by the Core, Implementation Tiers, or Profiles, and we have heard that some organizations have been unclear about how to execute these steps. We suggest including references to informational sources that could assist an organization to better understand the purpose of the steps as well as to assist them in performing the steps. Additionally, without a comprehensive Risk Assessment it would be very difficult to analyze a “Current Profile” and produce a “Target Profile.” NIST should consider providing guidance on how to conduct a Risk Assessment for those entities who are not as familiar with the concept.Finally, NIST should also examine whether the CSF appropriately recognizes the rapid growth in several technological areas, including software defined networks, the use of mobile devices to access virtual private networks, and the explosive growth of connected devices (often referred to as the Internet of Things or IoT).	
12	Are there additions, updates or changes to the Framework’s references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?	NIST should examine for inclusion the emerging standards and guidelines on the development and implementation of IoT into the enterprise. We have also heard concern from customers that if a specific control is not listed as an informative reference, it cannot be used in conjunction with the CSF. We recognize that NIST has stated otherwise in the CSF as a whole, but NIST should consider including a visual representation of this in the Framework Core itself.	
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	N/A	

#	Question Text	Response Text	References
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	We encourage NIST to examine whether the CSF needs to address more directly the need for strong authentication tools and mechanisms. The rapid explosion of the IoT and the development and use of low cost connected devices has increased the need for strong authentication practices. Conversely, while we do not discourage NIST from exploring areas such as Automated Indicator Sharing or Technical Privacy Standards, we urge NIST to examine existing government efforts in these areas to ensure that any CSF activities in them are not duplicative or, worse, conflicting. Finally, we applaud NIST for its efforts to inform international audiences about the CSF and the collaborative process that was used to develop it, and we encourage NIST to reach out to international partners for suggestions on how to increase international adoption of these collaborative processes or even the CSF itself.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	As a starting point NIST should continue the same collaborative approach that was used to develop the CSF. NIST should also make clear from the outset that it is updating the CSF and that its basic structure and approach will remain fundamentally unchanged. It is important that organizations using the CSF, or considering using it, can do so with confidence that they will not have to start the process over.	
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?	We developed our own mapping of the CSF to our products and processes and have largely used those.	
17	What, if anything, is inhibiting the sharing of best practices?	For the most part organizations are not hesitant to share best practices or to highlight approaches that have worked for them; doing so can be used as a market differentiator. With that said, where an organization gains a competitive advantage through the use of proprietary practices, the economic incentives do not align with the free flow of information. Finally, the simple volume of best practices, standards, and guidelines that exist can result in information overload and make it hard for an organization to determine what mix of approaches best suits its needs.	

#	Question Text	Response Text	References
18	What steps could the U.S. government take to increase sharing of best practices?	It would be helpful if the government would showcase agency or department use of the CSF or of instances where Federal entities were sharing or publishing their best practices. Leading by example could spur some activity in this area.The government should encourage the use of "Security Overlay Templates," such as those introduced in NIST SP800-53r4, to address a particular system, technology, or scenario. If an organization is already using an overlay, that organization could provide instructions for using it with the CSF. NIST could also include verbiage in the CSF to explain how an overlay could be used in conjunction with the CSF. Finally, NIST should encourage industry partners to publish overlays tailored to their unique requirements that could be useful to similarly situated organizations.	
19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?	The facilitation of a robust insurance market for cybersecurity related incidents would be the best mechanism for the collection and centralization of security related data as there would be a strong economic incentive to accurately compile control and breach information and analyze the same. Incentivizing cybersecurity insurance in exchange for data sharing would be the most efficient way for the US government to obtain information at which point it could share the information as deemed appropriate.	
20	What should be the private sector's involvement in the future governance of the Framework?	The private sector should continue to be trusted advisors in the development and governance of the CSF. However, because of the broad reach of the CSF it is important that an impartial third party maintain it and ensure that any changes are aligned with best practices *writ large* and not the particular interests of any one group or sector.	

#	Question Text	Response Text	References
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	At this time we believe it would be premature to transition the CSF to an outside organization. NIST is a neutral third party with a demonstrated ability to collaborate effectively with a broad spectrum of interested parties, and the CSF development process created a strong trust relationship between NIST and interested parties. Trust of this sort has to be earned - it cannot be simply "transitioned" to an outside organization. For that reason alone, premature transition of the CSF to another organization could slow the continued evolution and use of the CSF.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	See response to question 21.	
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	See response to question 21.	
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?	Transition could result in decreased usage of the CSF, and in particular new versions of it, if those using the CSF do not have full confidence in the new organization. It could also inhibit the continued evolution of the CSF if the private sector does not trust the process and devotes fewer resources to working on it. In order to avoid this, should NIST elect to transition the CSF, the process should be done slowly and deliberatively, with NIST continuing to play some role in CSF governance.	
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?	A transition partner or organization would have to maintain the credibility and efficacy of the CSF. To do so, this organization would need to be impartial, competent, drive consensus between cultures, and have the resources to operate on a global scale.	