Views on the Framework for Improving Critical Infrastructure Cybersecurity - EmblemHealth
Response Template

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	EmblemHealth is a health maintenance organization and health insurance company which is headquartered at 55 Water Street in Lower Manhattan, New York City. It is a $10 billion company with 3.4 million members. The NIST Cyber Security Framework is used as the primary guideline for assessing our Cyber Security posture and operations.	
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.	Responding as a Framework user.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Utilizing the framework as the baseline reference document to assess, plan, monitor and manage our Cyber Security program. We utilize data from the Framework to provide capability maturity reporting to the C-Suite and other internal management staff.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	The framework has proven effective as the baseline reference document in assessing our relative Cyber Security Posture. We are currently developing metrics aligned with the Implementation Tiers and our own risk and criticality measures.	
5	What portions of the Framework are most useful?	The mapping to the NIST controls as well as other controls.	
6	What portions of the Framework are least useful?		
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)?	Lack of a clear standard framework for Healthcare prior to 2016 creates ambiguity regarding what is the standard for Healthcare. Adoption of the NIST CSF as the primary healthcare standard would be beneficial and less confusing for non-technical executives.	
8	To what extent do you believe the Framework has helped reduce your cyber security risk? Please cite the metrics you use to track such reductions, if any.	We tracked our capability maturity utilizing the Forrester IT Security CMM model throughout 2015 as we made improvements to our IT Security posture and operations. The primary guideline for our improvements was the ISO standard, however, we created our own map of ISO to NIST so we could understand how we compared to NIST CSF. Utilizing the two guidelines help us in identifying any gaps or opportunities as we proceeded through 2015. For 2016 we will focus on the NIST CSF and the implementation tiers as our model.	
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 Cyber security Enhancement Act of 2014?	Adopt an existing standard, NIST CSF as the baseline for any regulatory requirements. If a minimum standard could be adopted that would allow health care companies to have a target that if reached would provide some guidance to the C-suite that the IT department had achieved the proper security level	
10	Should the Framework be updated? Why or why not?	The framework should be continuously reviewed and updated.	
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.	We need to work with the framework for a longer period of time before we can provide actionable feedback	

#	Question Text	Response Text	References
12	Are there additions, updates or changes to the Framework's references to cyber security standards, guidelines, and practices that should be considered for the update to the Framework?	We need to work with the framework for a longer period of time before we can provide actionable feedback. However, it would be useful if NIST could develop a formal capability maturity model focused on the tiers and other criteria that organizations could use to assess their maturity. We are going to develop an internal model as this has proven invaluable in executive presentation and discussion.	
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?	We would be interested in the feedback on this question as we are in our first year of working with the framework.	
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 need to work with the framework for a longer period of time before we can provide actionable feedback	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	A migration path should be provided with guidance on the suggested level of importance of the changes	
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 need to work with the framework for a longer period of time before we can provide actionable feedback	
17	What, if anything, is inhibiting the sharing of best practices?	In healthcare confusion over what is the baseline standard that everyone should utilize. Special interest groups with their own standards creates additional confusion.	
18	What steps could the U.S. government take to increase sharing of best practices?	Sponsor Healthcare focused Cyber Security workgroup. Provide a minimum standard for controls adopted that would be used to establish a health plan had done all the right things	
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)?	See above.	
20	What should be the private sector's involvement in the future governance of the Framework?	Participate on a governing committee.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	No. Independence is ideal. NIST should facilitate discussion with the private sector.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?		
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 21 above.	
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?	Don't agree with transition from NIST.	

#	Question Text	Response Text	References
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 cyber security standards, guidelines, and practices within the United States and globally?	Don't agree with transition from NIST.	