#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	BSI was the world's first National Standards Body. BSI helped shape many of the world's management systems standards, including the three most widely adopted for quality, the environment. health and safety and information security (ISO/IEC 27001). BSI has worked closely with NIST from the beginning and attended all of the original 5 workshops prior to launch and we continue to contribute regularly with new and innovative ideas. Our interest from the begining and still is international harmonization to ensure sharing and calibration of best practices as many of our clients are global in nature and want an holistic approach to cybersercurity. BSI is also a co-founder of ISO and the oldest Certifying Body. We assess and certify organizations against the international standards along with providing education and content.	
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 Subject Matter Experts but play a leadership role in many International and National Committees and associations and our customer base number 99,000 many of who are users and non-users of the framework.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	N/A	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	Working with our experts and clients we have seen that the framework integrates easily with standards such as ISO/IEC 27001 as an "add on" to strengthen the core ISMS.	
5	What portions of the Framework are most useful?	Framework Core and Profile	
6	What portions of the Framework are least useful?	Framework Tiers - Useful but needs more guidance on the meaning and the financial impact as you move up the scale along with the need to justify doing so.	
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)?		N/A
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.		N/A
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?	Suggest a more cross-functional task force that will include representative from industry and international and national standards bodies that will form a change control process that monitors for conflicts and measures the impact of the change(s).	
10	Should the Framework be updated? Why or why not?	If justified. Changing just for the sake of change is not valuable. Using the Change Management process as described in (10) would provide valuable oversite on this.	
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.	As mentioned in (6) the tiers need more guidance on the meaning and the financial impact as you move up the scale along with the need to justify doing so. We view this document as guidance, so only the core should be updated as necessary to keep in pace with changes in the standards and cyber security best practice.	

#	Question Text	Response Text	References
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?	Not at this time. While there are many other standards and guidelines out there, the current list is inclusive of what others are derived from.	
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?	Possibly the financial sector. That is not well represented here	
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?	Should be updated to reflect the changes as it goes hand in glove with the CSF	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Suggested changes should go through a change management process, approved with an RFI published to get comments. Once finalized, there should be a "transition" window (1 - 2 years for example) to allow organizations to evaluate the changes and impact and then justify the inclusion or exclusion of the additional/updated controls.	
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?	The cooperation and communication efforts by Adam and his team have been unprecedented compared to what we have come to expect in the past from some agencies. The sharing of information and availability of resources has greatly enhanced our ability in our quest for international harmonization.	
17	What, if anything, is inhibiting the sharing of best practices?	Our experience so far has been great cooperation by industry associations.	
18	What steps could the U.S. government take to increase sharing of best practices?	Not sure they need to do anything except continue to foster cooperation among industry and standards leaders.	
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)?	A call to action for formal case studies should be in order here with a consistent template. These can be posted for viewing on the NIST site. Provides recognition to those who have implemented the framework controls.	
20	What should be the private sector's involvement in the future governance of the Framework?	We believe the private sector should have a say just as they have had since its development, but there has to continue to be oversight by NIST.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Again, in our opinion there has to be some NIST oversight and any outside involvement would have to be by a not for profit organization to avoid conflict of interest.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	If there is going to be a transition it should be all or nothing with the oversight part of the formula.	
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?	As mentioned in 21 above, not for profit and preferably a multinational organization with deep standards experience and clout internationally to support the goal of international harmonization.	
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 see much disruption if done correctly and with the right organization and mentioned above. A international standards organization will already have the experience in this area and processes in place to maintain and support.	

#	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 cybersecurity standards, guidelines, and practices within the United States and globally?	See 24. It would be imperative that a experienced standards body be involved.	