#	Question Text	Response Text	
1	Describe your organization and its interest in the Framework.	Aerospace and Defense contractor to DoD	
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.	SME	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Guidance while determining the compliance of our network(s)	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	This is an excellent reference tool	
5	What portions of the Framework are most useful?	comparative charts that match CSC vs NIST, etc	
6	What portions of the Framework are least useful?	there is no update button that would refresh it on a regular basis	
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 governement req'ts are moving faster than the tool currency	
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.	not measurable at this 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?	Form a single body for the US gov't that has a singular standard system	
10	Should the Framework be updated? Why or why not?	Yes, ease of lookup and use is needed when researching controls	
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.	Keep it up to date, include the CIS CSC chart itself and make all areas linkable	
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?	yes, update it monthly	
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?	include all the Sarbanes-Oxley references that cross into IT	
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?	yes, keeping them synchronized would be a step forward	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	the ability to choose the date of the framework will allow you to roll fwd or backward in time based on control differences	
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?	not measurable at this time	

#	Question Text	Response Text	References
17	What, if anything, is inhibiting the sharing of best practices?	Time	
18	What steps could the U.S. government take to increase sharing of best practices?	use a poster like CIS CSC	
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)?	peer NIST and Infragard together	
20	What should be the private sector's involvement in the future governance of the Framework?	never leave them out of any policy establishement efforts	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Ensure the DoD CIO office is a review authority on every NIST document	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	N/A	
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?	N/A	
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?	Loosing central control of this effort is not in the best interest of the larger population that use them	
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?	You could include European ISO standard partners in a review-only capacity	