#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Alion Science and Technology is a large business founded in 2002. Alion has ISO 9001:2008, ISO 17025:2005, and CMMI Level 3 certifications as well as a Top Secret facility clearance. Our major customers include the Army Provost Marshal General, the Office of the Secretary of Defense, the Secretary of the Air Force, and the Defense Threat Reduction Agency. Over the last decade Alion has been regularly included among the Top 100 Defense Contractors in industry publications such as Military Training Technology, Defense News, and Washington Technology.	
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.	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).	Alion uses the the Framework to build cybersecurity checklists for use by government and industry security analysts within our proprietary CounterMeasures® software program.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	No comment	
5	What portions of the Framework are most useful?	No comment	
6	What portions of the Framework are least useful?	No comment	
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)?	For large organizations, the requirement to adopt the Framework all at once creates a roadblock to adoption because of the large investment this calls for in a short period of time. There ought to be a mechanism to certify geographically-separated sub-components of an organization and thereby support phased adoption.	
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.	No comment	
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?	No comment	
10	Should the Framework be updated? Why or why not?	No comment	
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.	No comment	
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?	No comment	

#	Question Text	Response Text	References
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?	No comment	
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?	No comment	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	No comment	
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?	No comment	
17	What, if anything, is inhibiting the sharing of best practices?	No comment	
18	What steps could the U.S. government take to increase sharing of best practices?	No comment	
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)?	No comment	
20	What should be the private sector's involvement in the future governance of the Framework?	No comment	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	No comment	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	No comment	
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?	No comment	
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?	No comment	
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?	No comment	