#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Paramount is specialized in information security and assurance process, providing security services & product business Cyber security framework will definitely enhance the companies security capabilities, business strategies is terms of spending, acquiring new knowledge and fulfil the client requirements	
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.	Subject matter expert	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Internal management and communication and vendor management	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?		
5	What portions of the Framework are most useful?	The Core framework should also include functions such as Analysis and investigation apart from identification, protect, etc., as these are key component of cybersecurity lifecycle	
6	What portions of the Framework are least useful?	Section 2.2 must be more elaborative with examples	
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)?		
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.		
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?		
10	Should the Framework be updated? Why or why not?	Yes, framework need to focus on critical areas and key mitigation plan such as perimeter defence strategies, requirement of high availability for critical infrastructure, single point of failure and surviving various attacks (such as DDoS)	
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.	1) Framework Implementation Tiers must be more detailed with illustrative examples 2) Awareness and training section must focus on training IT staffs who are the front end worriers and most vulnerable to sophisticated attacks 2) Mitigation strategies needs to be incorporated in terms of following: 1st line of defence, 2nd line of defence 3rd line of defence starting with what are these types and strategies to strengthen the controls protecting the same 3) Instead of giving references, actual controls or key extract of controls would be more helpful and provide quick references 4) Tips and Key points need to be included	
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?	Instead of giving references, actual controls or key extract of controls would be more helpful and provide quick references as it would help IT / security professionals quickly take key points for implementation	
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?	Sector wide implementation guides will be useful, but if only critical areas or case studies from those sectors are show cased	
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?		
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Can provide updates in form of appendix quarterly and half yearly and during annual review points are incorporated as part of framework	

#	Question Text	Response Text	References
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?		
17	What, if anything, is inhibiting the sharing of best practices?		
18	What steps could the U.S. government take to increase sharing of best practices?	By focusing on key areas, provide more insight to mitigation plans and practical scenarios	
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)?	Awareness among organizations regarding the sensitivity & criticality of cyber security practices and developing case study thus assisting other organizations overcome weakness; Also NIST must ensure high level of privacy and confidentiality	
20	What should be the private sector's involvement in the future governance of the Framework?	Knowledge sharing is the key for improving any security framework	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Subject matter experts must be consulted in some of the areas	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	Informative references and 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?	Specialized organizations	
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?		
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?		