#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	We are interested in operationalizing the framework to help organizations more easily implement the framework within their organizations.	
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).	We will soon be mapping ISO 27001 results to the CSF for risk and compliance management. We are also reviewing for vendor management.	
4	What has been your organization’s experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	The concept of Tiers is not intuitive. It's not clear how Tiers should be implmented.	
5	What portions of the Framework are most useful?	**Core structure**. Logical and easy to understand. Offers transparency and traceability.	
6	What portions of the Framework are least useful?	**Tiers.** It's not clear how to best implement this concept.	
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)?	Some organizations don’t know how to get started. They require some level of implementation guidance.	
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.	TBD	
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?	Additional mapping of regulatory requirements (PCI, HIPAA, emerging 800-171 CUI, FFIEC, etc.) to the framework	
10	Should the Framework be updated? Why or why not?	Yes, to improve upon the great benefits already offered by the framework.	
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.	Assuming Tiers can be better explained, nothing should be removed. Proposed modifications/additions: **1)** Tiers implementation/use/benefit should be better explained. **2)** Additional standards/controls/regulatory requirements should be mapped to the framework. **3)** Expansion of profiles to include interim acceptable profiles as an organization progresses from an unacceptable Current Profile to an objective Target Profile **4)** Implementation guidance (e.g., use cases, how to get started, what implementation looks like, how to maintain once implmentation is complete) should be appended to the framework document.	
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?	Minimally 800-171 (CUI), PCI DSS, and HIPAA. A cross reference to the new FFIEC would also be helpful.	
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?	Department of Energy is one noteworthy example.	http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

#	Question Text	Response Text	References
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?	There are at least three roadmap items that appear tightly coupled to the framework for the purpose of continued framework advancement and adoption. As such, developments in these area should be communicated as part of any framework updates. Specifically, 4.3) Conformity Assessments, 4.6) Fed Agency Alignment (to help avoid duplication of effort with other simailar frameworks like RMF), 4.7) International Aspects, Impacts, and Alignment (to help multinational companies adopt the NIST CSF)	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Communicate regularly with industry/users to explain proposed updates. Work together to devise ways to minimize disruption.	
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 yet. More implementation guidance is needed, which is one of the recommendations we are making in this RFI response.	
17	What, if anything, is inhibiting the sharing of best practices?	Potentially many things: lack of incentives, liability concerns, competitive concerns.	
18	What steps could the U.S. government take to increase sharing of best practices?	Not sure. Perhaps this is the role of ISACs and IASOs.	
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 response to item 18.	
20	What should be the private sector’s involvement in the future governance of the Framework?	Support NIST in evolving the framework over time, as needed.	
21	Should NIST consider transitioning some or even all of the Framework’s coordination to another organization?	We believe that the the framework should continue to be managed by NIST with coordination and input from industry, similarly to how the original framework was developed.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	If anything, perhaps other regulatory content (controls/references) that are mapped to the framework (PCI, HIPAA, FFIEC, etc.)	
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?	Not sure.	
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?	Preventing disruption is one very good reason for NIST to maintain responsibility of 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?	Not sure.	