#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	State of Michigan. Department of Technology Management & Budget (DTMB). Comply to an industry standard framework as the foundation for the DTMB's Security Program.	
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.	The State of Michigan is a user of the Framework (DTMB and all Agencies). The Michigan Cyber Security team is a Subject Matter Expert in 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).	Ultimately, the end goal is to comply with all domains of the NIST Framework (i.e. Organizational, Technical, Administrative)	
4	What has been your organization’s experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	State of Michigan is in the process of implementing the Core Framework in 2016.	
5	What portions of the Framework are most useful?	Controls are well written and detailed.	
6	What portions of the Framework are least useful?	Instructional guidelines are lacking details. Lacking executive level language and presentation.	
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)?	Yes - Requires significant awareness and education for non-technical stakeholders across the organization which hinders 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.	We monitor the Reduction of number of Incidents/per Month	
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?	Yes - By utilizing a tool such as LockPath to track Governance, Risk and Compliance (GRC), to de-duplicate the regulatory process and to maintain compliance to current standards.	
10	Should the Framework be updated? Why or why not?	Framework must keep up with technology and threats to stay relevant in the current environment. (E.g. Address Internet of Things (IOT)).	
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.	Further refine summary and executive level documentation. Add Implementation Plan and/or Roadmap (further detailed).	
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 - Further cross reference again other frameworks (all standard framework sources).	
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?	Yes - Publish a synchronization implementation guideline against other frameworks.	
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. Weigh the new developments against a Risk Ranking process.	

#	Question Text	Response Text	References
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Publish the differences/changes as versions are published. Whenever possible, update Controls vs. Adding and Deleting to minimize change management. Periodic/scheduled updates to the Framework so organizations can plan and prepare.	
16	Has information that has been shared by NIST or others affected your use of 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?	Yes - UCF's ability to cross reference has enabled more efficient implementation of NIST. ISO 2700 was the starting point structure which allowed more efficient implementation of NIST.	
17	What, if anything, is inhibiting the sharing of best practices?	A culture of Silo's inside both technology and business units hinders enterprise adoption.	
18	What steps could the U.S. government take to increase sharing of best practices?	Mandatory compliance to NIST (or other industry standard) e.g. Federal Contract Requirement. Offer Grant money to pay for compliance	
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)?	Centralized repository for Lesson's Learned, Best Practices, Tool Reviews, etc. Additional conferences and forums available to public and private users.	
20	What should be the private sector's involvement in the future governance of the Framework?	Private sector should have input throughout the lifecycle of the Framework updates.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Yes - It would be extremely difficult not to introduce commercial gains and hinder best practices by transitioning to another organization. If there was a transition, an oversight entity would be still needed.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	Methodologies - So the implementation can be adopted by real world commercial implementations.	
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?	Preferably multi-national as NIST is very US centric. Organization or multiple organizations that have limited commercial gain at stake.	
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?	Introduce complexity by increasing the number of players in the life cycle. Publish the differences/changes as versions are published. Whenever possible, update Controls vs. Adding and Deleting to minimize change management. Periodic/scheduled updates to the Framework so organizations can plan and prepare. Contact/Feedback mechanism to the transitioned to entity.	

#	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?	Multi-national entity Potential minimal commercial gains Globally available infrastructure capabilities Expert experience in implementing NIST controls in a variety of lines of business and types of businesses "Hands on practitioners" on staff vs. high level consultants and researchers.	