#	Question Text	Response Text	References	References
1	Describe your organization and its interest in the Framework.	The Global Institute for Cybersecurity + Research (GICSR), headquartered at NASA/Kennedy Space Center, Florida represents a trusted international collaborative facilitating open dialogue, critical insight and through exchange linking critical infrastructure stakeholder to define and deliver scalable, flexible and adaptable cyber resilience solutions. GICSR is private-sector led in partnership with NASA/Kennedy Space Center and works in collaboration with the U.S. Department of Homeland Security, the U.S. Department of Derense, NIST, federal agencies, SLTT, and critical infrastructure owners and operators. Deborah Kobza, GICSR President/CEO has supported the development of the NIST Cyber Framework effort. GICSR is facilitating an international collaborative initiative, The Global Forum to Advance Cybersecurity, focused on operational guidance to manage mission-driven, cyber resilient services through the identification and implementation of best practices and lessons learned. Leveraging the NIST Cyber Frameworks (Framework for Improving Critical Infrastructure Cybersecurity, the NIST National Cybersecurity Workforce Framework (NIST), the NIST Framework for Cyber-Physical Systems; and the Department of Defense Enterprise Service Management Framework (DESMF) to operationalize cyber resilience via the integration of service management and cyber resilience. We will take advantage of the public tax payer and private sector investment in the basic lexicon called out in the DESMF. There are over three million people certified in the lexicon and millions of others who have been trained without certification. The Global Forum's purpose is to provide organizations , critical infrastructure sectors, and sub-sectors with a "disciplined" management approach, the "Critical Infrastructure Service Management Action Plan - CISMAP" - operationalizing the NIST Cyber Framework and cyber resilience enterprise-wide.	**DESMF**:http://www.rightexposure.com/desmf-ii-and-iii/ **Basic Lexicon of the DESMF**: www.axelos.com/itil	
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 Global Forum includes organizations from public and private sectors with a comon approach to the foundation of IT Service Management. Please feel free to ask about who is participating. .		
3	**If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).**	The Framework is leveraged to: Communicate a cybersecurity structure, Build upon organizational internal and external communications, Enable adoption and development of cyber security best practice policies, procedures and vendor requirements, Support CIO and CISO communications to other C-Suite roles and responsibilities, and Act as a foundational element in further definition of operational guidance within the context of cyber resilient mission driven IT services via the integration of IT service management and cyber resilience best practices.		
4	What has been your organization’s experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	The representation of the Forum members from multiple Critical Infrastructure Sectors gives us the ability to take advantage of a broad set of subject mater expertise and provide all interested parties with Sector specific targeted profiles.		
5	What portions of the Framework are most useful?	The Framework supports the ability for an organization to determine their Current Profiles (Current State).		

#	Question Text	Response Text	References	References
6	What portions of the Framework are least useful?	The Framework doesn't support defining what is required in the "Target Profile" to achieve desired cybersecurity risk goals. The Forum takes the NIST Framework to the next level by operationalizing cyber resilience and defining sector-specific Target Profiles.		
7	Has your ogranizations use of the Framework been limited in any way? If so what is limiting the use of the Framework (eg sector circumstance, organization factors, Framework features, lack of awareness)?	The Gobal Forum will help organizations to be aware of the Frameworks value to help them utilize its value.		
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.	N/A		
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?	Regulatory Harmonization.		
10	Should the Framework be updated? Why or why not?	The Global Forum will make suggestions for updates to the Framework with associated lessons learned for its continual improvement		
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.	The Global Forum will provide feedback to the NIST from its members on an ongoing basis based on Sector specifice utilization.		
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?	The Global Forum supports the Framework in the context of IT Service Management and the utilization of other best practices and Frameworks. We will provide feedback to the NIST.		
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?	The Global Fourm is is providing Sector and Sub-Sector specific Critical Infrastructure Service Management Action Plans (CISMAP) to operationalize the Framework		
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 in these areas: Cybersecurity Workforce, Federal Agency Cybersecurity Alignment, International Aspects, Impacts and Alignment, Supply Chain Risk Management.		
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Our Forum creates a way for people to share ideas and best practices, lessons learned utilizing a staged approach for introduction and release.		
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?	We are introducing a Forum for the public and private sector to collaborate in a way that will provide value to the participants by establishing a common context of ITSM satisfaction of intent vs conformance		

#	Question Text	Response Text	References	References
18	What steps could the U.S. government take to increase sharing of best practices?	Participation in our Forum helps break down long standing barriors between the public and private sectors and supports sustainable colaboration. Properly position the Framework on value vs conformance to standards. The Forum can help articulate the value to the public.		
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)?	The Global Forum to Advance Cyber Resilience		
20	What should be the private sector's involvement in the future governance of the Framework?	Governance of the Framework should come from the organization utilizing it. Guidance can come from participating in Forums like outs who have objectives to support governance language that is sector and organization specific		
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	NIST should maintain the core of the Framework and consider the input from Forums like our Global Fourm in support of general and sector specific updates.		
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?	N/A		
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?	N/A		