#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	SCRA is an applied research corporation with over 31 years of experience delivering technology solutions to federal and corporate clients and growing the knowledge economy in South Carolina. Within our portfolio of projects, SCRA integrated Framework core function activities within several SDLC processes for more efficiencies in meeting technical security requirements, compliance, and risk management.	
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.	Software Development/Sustainment SME and innovator of 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).	SCRA adapted within program management, development, and sustainment activities to meet client requirements. We used the Framework to standardize perspectives of security functions that, when executed concurrently and with full Team integration and awareness, yield optimized tools and process. By integrating core cybersecurity functions with software development processes/tools/best practices, we achieved efficiencies in meeting Government directed policies, instructions and compliance with negligable impact on operations, system maintenance and software improvements.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	Largely used the Core Framework and alignment to best practices and Government directed security requirements (e.g., STIG, NIST 800-53, DODI 8510 DIACAP, PCI, CJCSM 6510.01B Incident Handling)	
5	What portions of the Framework are most useful?	Core Functions matrix	
6	What portions of the Framework are least useful?	Privacy Methodology	
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)?	The Framework lends itself to improve communication across the Executive, Policymakers, Technical Implementers and CyberSecurity Auditors. There is room for improvement to communicate the security, ROI and risk-tolerance tradeoffs for which qualitative analysis is a powerful yet underutilized process.	
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.	The Framework has helped codify risk classification during information gathering, communication and assessment that improves program-wide risk awareness that corresponds to a reduction in risks.	
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?	See #10 Response below	
10	Should the Framework be updated? Why or why not?	Update to latest Federal governance and guidance. The Framework should be extended to provide more explicit, regulatory-driven measurable/observable benchmark/criterion which in turn would either recognize duplicative regulatory processes and/or deliberately re-inforce the necessary core function concurrent activities required to meet regulatory objectives. Rather than a checklist assessment, the framework should/could encourage objective-based evidence to look for, ability to demonstrate and assess efficiencies. Objective-based evidence matures the Framework from conformance for compliance checklist toward a relative risk-driven security posture with analytics for decision making.	
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 current framework with matrix may imply a silo'ed view of each core function that, when aligned to responsibilities and accountability roles, will likely be satisfied by disparate groups which stifles collaboration and weakens an overall cybsersecurity awareness posture. The framework should demonstrate and re-inforce the significance and importance of concurrent and continuous nature across all five functions. For example, the implementation of continuous monitoring technology addresses log auditing and detection. The benefits are amplified when the results are shared with the system architects and the software development team. The core functions should consider: Does the implementation include both centralized and distributed analytics?; What subfunctions should be laterally integrated to correlate and stratify findings from each team to provide a system-wide risk awareness?; Information sharing with penetration testing to strengthen test profiles aligned to raw data.	
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?	See #10 response	

#	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?	(blank)	
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. Demonstrative qualitative and quantitative performance statistics methods should be extended to the core functions. The Federal/Defense efforts in improvements in training, workforce, awareness, and checklist compliance performance metrics are notable, however these 'metrics' provide an incomplete perspective of the security vulnerability of the system and effectiveness of the program. Specific to a few framework roadmap listed development areas (Automated Indicators, Conformity Assessment, and Data Analytics); evidentiary metrics in dynamic behavior, usage, threat analytics mechanisms (both tools and process) are required to better understand the effectiveness of the cybersecurity program and inform decision makers.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	The Framework should remain voluntary and as a *framework*, provide common taxonomy and relationship/alignment to core functions and best practice references. As a best practice framework, organizations executing practices and activities towards regulatory compliance should face minimal disruptions. Updates should remain collaborative, consensus-built and no more than annually.	
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?	(blank)	
17	What, if anything, is inhibiting the sharing of best practices?	See #19 response	
18	What steps could the U.S. government take to increase sharing of best practices?	See #19 response	
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)?	An independently led consortia should tackle specific barriers that inhibit (or slow) cybersecurity 'information sharing'. Key inhibit issues to address should include reciprocity, legalities, independent assessment findings, and the lethargic vulnerability and patch notifications process.	
20	What should be the private sector's involvement in the future governance of the Framework?	(blank)	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	If so, the organization should be independent, non-authoritative, and maintain collaborative, consensus building consortia	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	(blank)	
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?	See response to #21	
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?	(blank)	
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?	See response to #21	