#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Clearwater Compliance specializes in Information and Cybersecurity Risk Management. We provide comprehensive, by-the-regulations compliance software and tools, risk management solutions, education and training, and professional services for organizations needing to understand where their risks are and what steps they can take to address them. Our interest stems from our comprehensive use of existing NIST standards as the foundation for our software and services.	
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.	Clearwater can be considered an SME in the information/cyber risk management domain. We have adopted the Framework as a NIST methodology for information risk management and cybersecurity implementation.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	We are developing a methodology and process to allow our clients to understand the fundamentals of the Framework and how to apply them to create or improve corporate cybersecurity programs.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	Clearwater Compliance has put the Framework into "production" in a systematic way that will allow us to offer a client a way to utilize the Framework components either in part or in whole.	
5	What portions of the Framework are most useful?	The Framework is a very useful tool but the implementation of the components is left to the users imagination. We have shuffled the components to put them in an order that makes programmatic sense to our clients.	
6	What portions of the Framework are least useful?	The voluntary use of the Framework without any real incentives to use it are inhibiting adoption.	
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)?	Interviews with some of our clients in the healthcare industry have indicated a lack of understanding of the Framework and no desire to engage otherwise. There is no incentive and they have bigger fish to fry. In many respects, this is considered yet another in a whole arsenal of risk management frameworks that are being promoted and it is all rather confusing (i.e. NIST SP800-37, 39, HITRUST, COBIT, etc.)	
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 key to this question is one of adoption. It appears the only organizations adopting the NIST CSF are government agencies and it doesn't appear to voluntary for them. We believe the Framework can work well to reduce cybersecurity risk assuming an organization has the commitment and incentive to do so.	
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?	It is imperative that the Federal Government ensure that individual agencies are not left to make their own interpretations of cybersecurity processes. The FDA can't be doing something different than the HHS. If they are, there needs to be an official arbiter who owns cybersecurity risk. To illustrate: if the CSF becomes a "standard" required by federal regulations and is made more prescriptive, each set of regulations will apply the same CSF standard.	
10	Should the Framework be updated? Why or why not?	Absolutely. The Framework is in real need of an implementation plan and an assessment tool like the Cyber Resilience Review (CRR) tool kit. Additionally, it needs to clarify it's place in the hierarchy of NIST risk management "standards."	

#	Question Text	Response Text	References
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 Implementation Tiers should be called a Maturity Model since that is what they are. A section that details how to implement the Framework is necessary. Implementation process using the Framework: 1. Leverage the framework but not in the order presented in the document 2. To implement the framework, start with the seven step implementation model. 3. Evaluate whether steps 3 and 4 should be swapped. 4. The implementation model would yield the information to document in the Framework Core. This would produce the “as-is” state of cybersecurity or “Current Profile” 5. The “Target Profile” would be established using the Implementation Tiers and the Risk Analysis to determine where to organization desires “to-be” in the future 6. Perform a gap analysis to establish the tasks necessary to achieve the target. 7. Document in a programmatic action plan such as a Plan of Action with Milestones	
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?	Framework references should come from sources that do not require payment to subscribe. They should be open source and authoritative.	
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 DOE C2M2 (Cybersecurity Capability Maturity Model); the DHS CRR (Cyber Resilience Review); NERC CIP (Critical Infrastructure Protection); SEI CMMI (Capability Maturity Model Integration)	
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?	They should. However, the Framework is in jeopardy of becoming a "paper tiger." If there is no mandate, incentive, penalty to using the Framework, it doesn't have any teeth. You may get organizations who really understand cybersecurity to adopt the Framework but it will be few and far between without some form of a requirement or regulation. Spending a significant amount of time on something unenforceable isn't productive.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	By keeping the fundamentals the same but adding additional value. Additional Functions in the Framework Core would be an example. The process model could swap steps 3 and 4 to ensure a risk assessment precedes a current profile.	
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 particularly.	
17	What, if anything, is inhibiting the sharing of best practices?	Market competition. A good cybersecurity program can be a market differentiator. Best practices should be developed by NIST in concert with industry and then codified for implementation by the federal government regulatory or oversight agency (i.e. HHS, SEC, etc.)	

#	Question Text	Response Text	References
18	What steps could the U.S. government take to increase sharing of best practices?	Establish a best practices baseline that is prescriptive regarding controls. Leverage existing NIST documents and external agency resources. Create a task force of government and industry to establish the baseline.	
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)?	Information Sharing Analysis Centers are a good means of doing this. Unfortunately, they are self-policed, cost money to join and don't have any oversight. Putting DHS in a position of establishing ISACs for critical infrastructure sectors could bring additional participants to the table.	
20	What should be the private sector's involvement in the future governance of the Framework?	Private sector involvement is continued development of the Framework is critical. They have the inside story on what is happening within any particular sector, what the inhibitors are, what the pain points are and are willing to contribute. Organizations like CHIME for healthcare are very involved and can add real value.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	No reason to do so. NIST is the keeper of the existing standards and should remain the "keeper" of the Framework.	
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?	Clearwater would prefer that NIST retain responsibility for the Framework but if it is decided to transition it, the Framework should be transitioned to an organization that is funded by the government or is in academia. For instance, CMMI is a solid program and many organizations are working diligently to get their CMMI certification. This is administered by Carnegie Mellon but was born out of a consortium of government and industry prior to being turned over to Carnegie Mellon. This type of cybersecurity "certification" (Level 1 - 5) would help to promote Framework adoption.	
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?	By keeping the fundamentals the same but adding additional value. Additional Functions in the Framework Core would be an example. The process model could swap steps 3 and 4 to ensure a risk assessment precedes a current profile. Make incremental improvements and not wholesale changes to minimize impact.	
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?	Clearly, ISO27000 is already positioned well to assume some or all of the reponsibilities. The problem is that none of ISO27K is mandated or required and it costs to get certified. No incentives are available around certification. It will be necessary that any organization that assumes reponsibility will need an incentive program to ensure organizations adopt a solid cybersecurity program founded on best practices.	