#	Question Text	Response Text	References
	https://www.federalregister.gov/articles/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity	This document has a comment period that ends in 54 days (02/09/2016)	cyberframework@nist.gov
1	Describe your organization and its interest in the Framework.	CyberEnginuity, LLC is a cybersecurity risk management training and consulting company. We assist large, medium and small organizations in designing and implementing cybersecurity programs. In particular, we promote the NIST CSF as the primary Framework for standards integration and 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.	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).	Consulting and advising services.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	Professional training in all areas.	
5	What portions of the Framework are most useful?	Profiles development	
6	What portions of the Framework are least useful?	NA	
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)?	While engaging customers in the gaming industry as a risk management consultant for cybersecurity framework design and implementation, the organizations view the NIST CSF as a US framework with potential government oversight. The organizations have a preference for established international frameworks such as ISO 27001/2. Their reasoning is that they are more favorably recognized by the international community when servicing guests and customers internationally. Their concern is that the NIST framework does not have this international notoriety.	
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.	Organizations are in the early stages of building knowledge about the framework. The government overatures of the framework slows the adoption by many private organizations. The ISO 2700 series and ITIL standards began as British government standards before transitioning into the international community, gaining global acceptance. This may be a model for the NIST framework to become ubiquitiously accepted.	
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?	A governance body consisting of a public/private partnership could be a measure to achieve this goal.	
10	Should the Framework be updated? Why or why not?	The framework itself should not be updated on a regular basis. The framework was designed to decouple the dynamic nature of cybersecurity from the framework architecture to provide stability to a broad base of organizations in a cost effect manner. Changes should only be made when such changes will improve the architecture in measurable ways.	
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.	Securing ecommerce is a key requirement and goal of the framework. More mapping is needed between the CSF and PCI DSS standards, SOX and related controls.	

#	Question Text	Response Text	References
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, PCI and SOX mapping.	
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 CSF implementation guide using the C2M2 can be a model for non-government organizations. Require implementation methodologies that are common to the private sector.	
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?	The focus could be on updating the roadmap on a regular basis, and not the actual CSF. Since the roadmap is impacted by future uncertainties, it can provide the flexibility for path correction.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Provide a website that is entirely devoted to the framework and impacts.	
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?	The NIST Cybersecurity website and DHS programs have been helpful. However the sites do not provide the detailed egineering view needed for implementers.	
17	What, if anything, is inhibiting the sharing of best practices?	Trust, and the competitive environment. Cybersecurity is still considered to be mostly an internal activity, surrounded by many types of sensitivies.	
18	What steps could the U.S. government take to increase sharing of best practices?	Steps taken by the government are quite often viewed as authortarian. However government are in the position to uniquely spur the CSF adoption through incentives. Cyber insurance underwritters can offer premium benefits to organizations that adopt the NIST framework.	
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)?	Communication directly to the C suites the benefit of information sharing and the new legislation to support this activity.	
20	What should be the private sector's involvement in the future governance of the Framework?	Continued collaboration with NIST as the convenier for the CSF.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Transitioning would have to be shifted to a neutral industry organizations such as ISO.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	The key concern is adoption and implementation. Therefore transitioning all of the framework is recommended.	
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?	Multinational organization using the BS7799 model. NIST could continue to maintain a US version of the framework for US consesus input to the international oversight. This is important since the framework is used by US government agencies. The United Nations cybersecurity division could be a forum for international cooperation and coordination.	
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?	In the event of an international transition, maintain a US working group. In the event of transitioning the framework to a US entity, ensure the entity is a neutral party.	

#	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?	This role may be best fulfilled by an organization that is already a key player in the international community. One that has be well established over several decades. For example ISO, and UN. Other models may be collaboration between national standards organizations.	