Docket Number 151103999-5999-01		RFI Response by Huawei Technologies USA	4-Feb-16
#	**Question Text**	**Response Text**	**References**
1	Describe your organization and its interest in the Framework.	Huawei is a global leader of ICT solutions for telecom carriers, enterprises, and consumers. Huawei's telecom network equipment, IT products and solutions, and smart devices are used in 170 countries and regions. Huawei ranked 228th on the Global Fortune 500 based on its revenue in 2014. Cyber security is an issue of intense interest to Huawei's customers and governments, and vendors alike; it is a focus of Huawei and cyber security assurance is one of our core company strategies. We believe that the NIST Cybersecurity Framework can be a valuable tool for any organization to use to assess risk, regardless of what standards or best/good practices that organization may use or refer to for guidance, if any. The Framework gives organizations one element of what they need to do about the risk they face – a standard-neutral and vendor-neutral tool to assess their own risk and preparedness and give them guidance to chart a course toward a more appropriate security posture given their risk environment. It can also be used for helping an organization compare the risk posture of suppliers and business partners. We believe that the Framework can be a good starting point for any organization that wants to better understand, and improve, their risk posture. We worked closely and successfully with a tier-3 customer regarding application of the Framework to its operations informed by the CSRIC cyber security best practices and regarding what Huawei as a supplier is doing to address supplier supply chain risk. This is important because organizations of all sizes can find the prospect and possible cost of addressing supply cain risk daunting, but it is important for organizations of all sizes to address this risk so as to not leave those parts of the US critical infrastructure unprotected. Huawei has top-level, organization-wide commitments to address cyber security and privacy risks, commitments that are "owned" by the Board and C-level executives; (2) Huawei has enterprise risk-management programs that incorporate cyber security and privacy risks; (3) Huawei has an internal organization-wide governance structure to address cyber security and privacy risk, which provides visibility to the Board and C-level executives; (4) Huawei has implemented cyber security and privacy requirements and baselines, and performance metrics, which are associated with specific business groups and departments, and individuals; and (5) Huawei has implemented internal compliance, verification, and audit mechanisms to provide the ability to accurately assess risk status, compliance, and accountability, and provide visibility to the Board and C-level. 6) Huawei requires all of its subcontractors and supplliers to undergo a multi-point cyber security	

#	Question Text	Response Text	References
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).		
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	Worked with a customer to apply the entire Framework to its operations.	
5	What portions of the Framework are most useful?	Core.	
6	What portions of the Framework are least useful?	Tiers.	

#	Question Text	Response Text	References
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)?	No.	
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.		
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?		

#	Question Text	Response Text	References
10	Should the Framework be updated? Why or why not?	Update to include guidance regarding supply chain risk (as suggested in the NIST Roadmap) which is missing from the Framework and is a very important subject for guidance to users and buyers of ICT as well as to providers. Huawei believes that malicious damage may occur in all activities of the global supply chain, so it is important to focus not only on individual activities, but also the entire supply chain. Supply chain threats fall into two major categories: tainted products and counterfeit products. Threats that can cause tainted and counterfeit products include malware, unauthorized parts, unauthorized configuration, scrap sub-part parts, unauthorized production, and intentional damage. Because of the prevalence of vulnerabilities in networks and systems in the face of a wide range and high sophistication of malcious attackers, it is important to address supply chain risk to protect critical infrastructure, government services, the functioning of private organizations, and the privacy and integrity of proprietary and private information of organizations and individuals. Because of the importance and resonance of the NIST Framework in the United States and in many parts of the world, it would be very valuable to have the Framework give guidance about supply chain risk.	
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.	Update to include guidance regarding supply chain risk (as suggested in the NIST Roadmap).	
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?	Add reference to Open Trusted Technology Provider Standard (O-TTPS - ISO 20243) and CSRIC Cyber Security Best Practices.	http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

#	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?	CSRIC Cyber Security Best Practices for the telecom sector.	https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf
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?	Update to include guidance regarding supply chain risk (as suggested in the NIST Roadmap).	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Provide an overlay to the Framework that gives guidance for supply chain risk that is not likely to cause disruption.	
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?	CSRIC Cyber Security Best Practices for the telecom sector provides guidance regarding risk in the sector.	https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

#	Question Text	Response Text	References
17	What, if anything, is inhibiting the sharing of best practices?	Need greater leadership by government and major organizations working collaboratively, including through sector organizations (SCCs and GCCs).	
18	What steps could the U.S. government take to increase sharing of best practices?	Government needs to work with the private sector to drive more substantial progress in reducing risk and increasing preparedness. One concrete step would be for governmental and private industry leaders to communicate an executive message designed to identify and raise due diligence requirements for Boards and C-level executives regarding the need to understand their organization's cyber security and privacy risk and preparedness posture, and develop and implement a plan to move to a more appropriate and sustainable risk/preparedness posture. This message -- in appropriate instances communicated on a sector rather than national basis -- would include recommendations that organizations (1) need top-level, organization-wide commitments to address cyber security and privacy risks, commitments that are "owned" by the Board and C-level executives; (2) need to have enterprise risk-management programs that incorporate cyber security and privacy risks; (3) need an internal organization-wide governance structure to address cyber security and privacy risk, which provides visibility to the Board and C-level executives; (4) need to identify and implement cyber security and privacy requirements and baselines, and performance metrics, which are associated with specific business groups and departments, and individuals; and (5) need to implement internal compliance, verification, and audit mechanisms to provide the ability to accurately assess risk status, compliance, and accountability, and provide visibility to the Board and C-level. This executive message should include a recommendation that organization use the NIST Cybersecurity Framework -- sometimes characterized, quite appropriately, as "a risk analytic tool" --- or a similar analytic approach, to assesss their risk, identify a target risk posture, and develop a plan to reach that target risk posture. Huawei has taken each of the steps detailed above. In addition, government should work with private sector to encourage private industry through Sector Coordinating Councils and the Cross-sector Cyber Working Group, or other formal or informal groups, to leverage their collective purchasing to drive greater availability of more secure products and services by (1) identifying common security requirements for products and services; (2) encouraging buyers to be more consistent in using security requirements in their procurements; and (3) encouraging buyers with similar requirements to work collaboratively incentivize providers to raise the bar on cyber security and assurance. There is perhaps no greater incentive to motivate providers to raise the bar than the desire to sell their products and services. Not enough is being	The EastWest Institute EWI is working with key companies (Huawei and Microsoft and others) and governments (US, China, Russia, UK, Germany, India, etc.) to seek agreement on contentious cyber issues including promoting the global availability and use of more secure ICT products. http://www.eastwest.ngo/info/increasing-global-availability-and-use-secure-ict-products-and-services; http://www.eastwest.ngo/cyber. To incentivize producers of ICT products and services to provide more secure products, Huawei launched the Top 100 Requirements to encourage buyers of ICT products to be more informed, consistent, and organized regarding what they should ask of, or require from, their vendors/suppliers. http://www.huawei.com/en/EBG/Home/news/global/2015/201511130951.

#	Question Text	Response Text	References
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)?	Expand the PCII (Protected Critical Infrastructure Information) provisions to allow other agencies (e.g., FCC, Treasury, Energy, FERC/NERC) in addition to DHS to provide similar confidentialilty protection for the information provided by the private sector.	
20	What should be the private sector's involvement in the future governance of the Framework?	Same role that it has been providing as active stakeholder(s) in the public-private partnership with NIST.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	No. No formal transitioning is required. Private sector can do with CSRIC did; provide customized guidance for sectors/sub-sectors (and for multiple sectors when there is similarity that warrants it).	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	No transitioning required; private sector entities can share metholodogies that are appropriate for particular sectors, sub-sectors, and cross sectors.	

#	Question Text	Response Text	References
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?	Not applicable.	
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?	Not applicable.	
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?	Not applicable.	