Organizational Information	**Response**
Organization Name	The Open Group - The Open Group Trusted Technology Forum (OTTF) and The Open Group Security Forum.
Organization Sector	Standards and Certification Development Organization - Member driven consensus based standards for IT
Organization Size	The Open Group: Staff 70, Member Organizations 500, Member Participants 40,000
Organization Website	The Open Group: http://opengroup.org The OTTF: http://opengroup.org/subjectareas/trusted-technology
Organization Background	**The Open Group** is a vendor and technology-neutral consortium, operating as “not-for-profit”, with over 27 years of experience, formed through the merger of X/Open Company Limited and the Open Software Foundation. It has offices in San Francisco (USA), Boston (USA), Reading (UK), Tokyo (Japan), Johannesburg (SA), Paris (France), and Shenzhen (China). It has over 500 member organizations, with over 40,000 participants in The Open Group activities from over 95 countries. **The Open Group Trusted Technology Forum** is a forum of The Open Group focused on product integrity and supply chain security standards and certification programs for COTS ICT providers - to mitigate the risk of tainted and counterfeit components and products. **The Open Group Security Forum** develops standards and best practices in information security management, security architecture, and risk management.
Point of Contact Information	**Response**
POC Name	Sally Long
POC E-mail	s.long@opengroup.org
POC Phone	978-835-2671

#	Question Text	Response Text	References
	Describe your organization and its interest in the Framework.	**The Open Group** is a vendor and technology-neutral consortium, operating as "not-for-profit", with over 27 years of experience, formed through the merger of X/Open Company Limited and the Open Software Foundation. It has offices in San Francisco (USA), Boston (USA), Reading (UK), Tokyo (Japan), Johannesburg (SA), Paris (France), and Shenzhen (China). It has over 500 member organizations, with over 40,000 participants in The Open Group activities from over 95 countries. **The Open Group Trusted Technology Forum** is a forum of The Open Group focused on product integrity and supply chain security standards and certification programs for COTS ICT providers - to mitigate the risk of tainted and counterfeit components and products. **The Open Group Security Forum** develops standards and best practices in information security management, security architecture, and risk management.	For more information on The Open Group, visit the home page: http://opengroup.org
	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 Open Group Trusted Technology Forum and The Open Group Security Forum could be classified as a subject matter expert. They are comprised of multiple organizations (from government, industry, and 3rd party evaluators), some of which are using and some of which are not using the Framework, but all of which are involved with cybersecurity and supply chain security in their organizations. This RFI response from The Open Group does not represent a consensus view from the member organizations' individual or collective official opinions.	For more inforation on The Open Group Technology Forum, please visit the Forum website at: http://opengroup.org/subjectareas/trusted-technology
	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	N/A - The Open Group in its role as a technology-neutral consortium (See #1 and #2) does not use the Framework, though some of our members may. The Forum focuses instead on cybersecurity and supply chain standards and best practices for ICT providers.	
	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	SEE #3	
	What portions of the Framework are most useful?	SEE #3	
	What portions of the Framework are least useful?	SEE #3	

#	Question Text	Response Text	References
	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)?	SEE #3	
	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.	SEE #3	
	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?	The standards referenced by the Framework should not be called out by law or policy as mandatory. However acquisition guidance related to a recommended list of open standards/best practices could be helpful to acquirers and providers alike; to acquirers so they understand better what they could be asking of their providers/suppliers and to providers to understand better what standards/best practices they should be following in terms of product integrity, and cyber and supply chain security. In order to provide that acquisition guidance and make such recommendations it is important to understand which standards apply to various areas; for example, which standards/best practices apply to: technical protocols, to operational processes or to product integrity and supply chain security. All are essential. A better approach might be to provide options for **existing** standards/best practices in the various areas - as acquisition guidance - instead of running the risk of re-inventing what already exists and regulating it.	
	Should the Framework be updated? Why or why not?	Yes, the Framework should be updated to account for best practices on product integrity and supply chain security. As the EO indicates, where other standards exist we should not re-invent them - please see the response below for specifics.	The Open Trusted Technology Provider™ Standard -(O-TTPS) - Mitigating Maliciously Tainted and Counterfeit Products (Technically identical to ISO/IEC 20243:2015) - is freely available from The Open Group Bookstore here: www.opengroup.org/bookstore/catalog/C147

#	Question Text	Response Text	References
	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.	NIST should add coverage for supply chain risk (potentially as an overlay or an appendix to the Framework) - and it should cover the risk of taint and counterfeit parts and products. There are existing standards that should be referenced for supply chain and trusted technology providers (e.g. ISO/IEC 20243:2015, technically equivalent to the Open Trusted Technology Provider Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products published by The Open Group). This is a set of best practices for COTS ICT providers that address product integrity and supply chain security throughout a product's life cycle (from design through disposal, both in-house and out-sourced) including the supply chain. The standard was developed over 5 years of consensus building in a partnership with some of the most mature vendors in the industry in collaboration with government.	The ISO/IEC 20243:2015 standard (technically equivalent to the O-TTPS) is available from ISO for a fee to ISO here: http://www.iso.org/iso/home/search.htm?qt=20243&active_tab=site&published=on
	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.	In addition, this input represents a standard recommendation from The Open Group Security Forum staff: They have seen widespread adoption by large organizations in critical infrastructure sectors of the Open FAIR standards (O-RT and O-RA) as a methodology with which to measure and quantify cybersecurity risk. The NIST CSF could be enhanced in the core (ID.RA section), implemention tiers, and informative references by adding mention and use of Open FAIR. The O-RT document provides a standard definition and taxonomy for information security risk, as well as information regarding how to use the taxonomy.<PLEASE NOTE - It was neccesary to add an additional row for repsonding to this question to allow us to include a link to an additional standard: FAIR O-RT in column D. Excel does not seem to allow 2 hyperlinks in the same cell>	Open FAIR O-RT https://www2.opengroup.org/ogsys/catalog/C13K
	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.	In addition, this input represents another standard recommendation from The Open Group Security Forum staff. This document is The Open Group Standard for Risk Analysis (O-RA), which provides a set of standards for various aspects of information security risk analysis. It is a companion document to the Risk Taxonomy (O-RT) Standard (C13K). <PLEASE NOTE -It was neccesary to add an additional row for repsonding to this question to include a link to an additional standard: FAIR O-RA in column D. Excel does not seem to allow 2 hyperlinks in the same cell>	Open FAIR O-RA: https://www2.opengroup.org/ogsys/catalog/C13G
	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, there are additions that should be considered. The Framework should be updated to account for best practices on product integrity and supply chain security. The Framework is written primarily from an operators perspective and does not sufficiently address requirements/recommendations for providers who supply the products to the critical infrastructure operating environment. That is, best practices that ICT providers should be following to mitigate the risk of tainted and counterfeit parts, while the products are being designed, developed, manufactured. References to best practices for product integrity and supply chain security are missing - they should be added.	

#	Question Text	Response Text	References
	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?	Yes, in terms of product integrity and supply chain security, please note the approach taken by The Open Group members. The members defined, by consensus, an international standard of best practices: The Open Trusted Technology Standard - Mitigating the Risk of Tainted and Counterfeit Products (O-TTPS), which was submitted to ISO as a PAS submission and was approved by ISO/IEC as ISO/IEC 20243:2015. The standard was developed for use by COTS ICT providers and applies to all constituents in the ICT supply chain: OEMs, hardware and software component suppliers, integrators, value-add resellers and distributors. Additionally, expanding on this approach, The Open Group developed an Accreditation Program, which identifies providers who conform to ISO/IEC 20243 as Open Trusted Technology Providers by listing them on a public registry. This approach not only allows acquirers to identify accredited integrators and OEMS to partner with, but it also allows OEMs to identify accredited hardware and software component suppliers, distributors and resellers with whom the OEMs can chose to partner. Any sector or any Cybersecurity Framework implementer that relies on ICT for their operation can take advantage of this existing approach by recommending their ICT providers adopt the ISO/IEC 20243:2015 standard.	The O-TTPS Accreditation Program website, which helps assure conformance of ICT providers to the ISO/IEC 20243:2015/O-TTPS, can be found here: http://opengroup.org/accreditation/o-ttps
	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. Supply chain was one of the nine areas identified in the Roadmap and it is important that the Framework be extended to include references to supply chain standards (potentially as an overlay or an appendix to the Framework).	

#	Question Text	Response Text	References
	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	For supply chain we suggest a two-pronged approach: 1) First update the NIST Cybersecurity Framework (CSF) with specific references, when there are specific points of interfaces with suppliers, and where existing supply chain standards like ISO/IEC 20243 apply. The Open Group has published an Implementation Guide that demonstrates how the Open Trusted Technology Provider™ Standard (O-TTPS) (recently approved as ISO/IEC 20243:2015) can address the supply chain best practices relevant to the CSF - and identifies those specific interfaces. The Guide also identifies some gaps, in that the CSF is written primarily from an operational perspective; what owners/operators should do within their operations. While that perspective is critically important it also illustrates the basis of the supply chain gap. To further eliminate the risk of tainted and counterfeit component/products from their environments, implementers of the CSF should consider working with providers who are conforming to best practices like those defined in ISO/IEC 20243. ISO/IEC 20243 defines what IT providers should do throughout their product development life cycle - from design through disposal (both in-house development and outsourced development) - **before** the products or h/w and s/w updates are installed in critical infrastructure operating environments. 2) To address the supply chain gap in the CSF more directly, we also suggest it would be worth adding an appendix, which identifies the standards and in some cases, as with the O-TTPS (ISO/IEC 20243) the certification programs to identify providers that conform to the standards. This appendix could address more directly, what CSF implementers could be asking of or recommending to their providers to help assure their providers are consistently following cyber and supply chain best practices including mitigating the risk of tainted (e.g. malware capable or malware enabled) and counterfeit components.	The Open Group Framework Implementation Guide identifies some supply chain gaps and specific supplier interfaces where SO/IEC 20243 applies. It is also freely available from The Open Group site here: https://www2.opengroup.org/ogsys/catalog/G151
	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?	SEE #3	
	What, if anything, is inhibiting the sharing of best practices?	SEE #3	

#	Question Text	Response Text	References
	What steps could the U.S. government take to increase sharing of best practices?	SEE #3	
	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)?	It is essential that standards, frameworks etc. be evolved through lessons learned once put into practice. This type of program needs to exist as long as the sharing makes a difference in the evolution. It is important that it not just be a talk-shop initiative, it needs to be results oriented or at least tied directly back to the results organization who evolves the Framework.	
	What should be the private sector's involvement in the future governance of the Framework?	Private sector is critical for practical input.	
	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	We believe NIST is the appropriate organization to coordinate the Framework. However, if a transition is deemed appropriate and a strategy for such progresses, The Open Group would be very interested in being involved in those discussions.	
	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	SEE #21	
	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 #21	
	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?	SEE #21	

#	Question Text	Response Text	References
	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 #21	