#	Question Text	Response Text
1	Describe your organization and its interest in the Framework.	The Utilities Telecom Council (UTC) is a global trade association that focuses on information and communications technology (ICT) challenges for utilities and other critical infrastructure industries. UTC's members range from large investor-owned utilities to small rural electric cooperative utilities and municipal utilities. UTC members also include providers delivering ICT products and services to utilities. UTC has been an active participant in the NIST Cybersecurity Framework process. In addition to contributing to the Framework itself, we have continuously made our membership aware of the Framework's benefits and have worked with UTC members to use the NIST Framework to establish, assess, or improve their cybersecurity programs.
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.	UTC is responding as a representative of multiple utilities and as a 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).	UTC members use NIST Framework in a variety of ways. Utilities with mature security programs use the NIST Framework to validate their existing programs and determine if they have any current gaps. Utilities that are establishing security programs use the Framework to understand what they need to include in their security program. Utilities use the Framework as the basis for assessing their security programs and identifying areas for improvement; to communicate with their suppliers, and to communicate results to senior leadership. A number of UTC members use the NIST Framework in combination with other cybersecurity frameworks, such as Cybersecurity Capability Maturity Model (C2M2) and NIST Special Publication 800-53.
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	We see UTC member utilities using the Framework in a variety of ways. In our observation the Core is the most used part of the Framework, followed by the Profiles. For example, UTC members find the Framework Core useful in defining the universe of control objectives that comprise a health of a cybersecurity program and for identifying gaps in their current cybersecurity programs. We see some use of the other portions of the Framework but not nearly as much as the Core.
5	What portions of the Framework are most useful?	Different organizations use the Framework differently. It is hard to tell what is most useful and what is not. However, we are able to point out that the most **used** portion of the Framework is the Framework Core. While the Framework Core does not present any new concepts, it provides a birds-eye view into all relevant content. It is useful to have such content in one place for efficiency and convenience of a busy security practitioner.
6	What portions of the Framework are least useful?	Different organizations use the Framework differently. It is hard to tell what is most useful and what is not.

#	Question Text	Response Text
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)?	Many UTC member utilities have had little chance to consider the NIST Framework due to the fact that the vast majority of their cybersecurity time and resources are dedicated to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Version 5 transition. However, under the auspices of the NERC Critical Infrastructure Protection Committee (CIPC), a group of electric utility industry cybersecurity experts mapped NERC CIP Version 5 requirements to the NIST Framework Core and C2M2. Some utilities use this mapping to guide their efforts to develop security practices that meet both NERC CIP Version 5 requirements and NIST Cybersecurity Framework. Additionally, the Energy Sector Cybersecurity Framework Implementation Guidance provides guidance on implementing the Framework through implementing C2M2.
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.	NERC CIP Version 5 transition activities have helped put a spotlight on cybersecurity within utility organizations. Using NIST Cybersecurity Framework to assess and establish cybersecurity programs has a similar effect. Having more attention on cybersecurity contributes to risk reduction. No metrics are available at this point.
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?	Greater outreach to Federal (including independent agencies), State, and local regulators, is required to help alleviate the creation of regulations that are duplicative or conflicting with the current processes and/or with the Framework. Such outreach may have many forms including individual meetings, conferences, facilitated workshops, and other means. Collecting and making available industry case studies and sharing those with the respective regulators could also benefit this process.
10	Should the Framework be updated? Why or why not?	The electric utility industry has had experience developing and implementing several versions of NERC CIP standards. This experience demonstrated that it is critical to have a period of stability to enhance, optimize, and measure security programs vis-à-vis applicable standards. The Framework is still relatively new to many smaller utilities with less mature security programs. While some utilities have found it a useful tool, others have not had a chance to take full advantage of it. Utilities are currently using the Framework to establish their security programs and need time to get used to it, monitor and measure results, and get the full benefit from its implementation. Changing the Framework this early in the process will confuse those using it. Changing the Framework now will also interfere with the organizations' ability to compare their cybersecurity programs "before" and "after" with the goal of measuring their performance against the Framework. Finally, more experience using the Framework will help produce useful feedback for future Framework revisions.

#	Question Text	Response Text
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 Framework itself should not be changed due to the reasons elaborated in Question 10. However, further guidance for how to use the Framework is needed for smaller and medium-sized enterprises. While larger UTC members have established cybersecurity programs and have used the Framework to **validate or enhance** their programs, the smaller companies, with rare exceptions, have used it to **establish** their cybersecurity programs. In many UTC member utilities individuals charged with developing and implementing these programs are not cybersecurity practitioners, but have other (mostly technical) backgrounds. Network engineers, IT architects, power engineers, compliance experts, and such are learning about cybersecurity through implementing NIST Cybersecurity Framework in their respective organizations. They need further guidance about how to best use the Tiers, what the Core means within their environments, and which informative references to turn to for additional detail within their respective contexts. Implementation guidance for smaller organizations is critical for raising the bar of cybersecurity in the Nation. However, this implementation guidance should be specific and concise, and does not have to be fully comprehensive (like NIST special publications) to help those using it with relevant information. This implementation guidance should not be added to the Framework but be provided in separate document(s), in support of the Framework. Additionally, some perceive the NIST Cybersecurity Framework as something entirely new and needing to be done in addition to or on top of the existing cybersecurity programs, even those based on existing standards and guidelines that precede the NIST Framework (e.g., ISO/IEC 27001). There is a general misperception that new standards are still required while there are hundreds of standards corresponding to individual NIST Framework subcategories or groups of subcategories. NIST has an opportunity to help the community identify existing standards, guidelines, and selected best practice documents that correspond to individual subcategories or categories. This can be done by creating lists of relevant standards and cataloging them on the cscrc.nist.gov/cyberframework/ tagged to the specific categories and subcategories. This would essentially create additional informative references per Category and perhaps Subcategory that the community could look into for information about how to implement these specific categories and subcategories.
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?	There is one very important omission in the informative references that UTC has noted before. The Framework is only mapped to ISO/IEC 27001 **controls** located in ISO/IEC 27001 Annex A. However, it is the numbered clauses in ISO/IEC 27001 that provide critical **processes** that enable cybersecurity. ISO/IEC 27001 numbered clauses were not mapped to the original version of the Framework. Mapping to ISO/IEC 27001 clauses has several substantial benefits. First, it will assist organizations using ISO/IEC 27001 in validating their security programs against the Framework. Second, it will demonstrate to the international community how the Framework relates to the globally accepted and broadly used cybersecurity standard, ISO/IEC 27001, which could help increase the use of the Framework use globally. Third, it will help demonstrate "completeness" of the Framework vis-a-vis a mature risk-based and process-based standard. This proposed update is limited to adding

#	Question Text	Response Text
		ISO/IEC 27001 processes to the Framework Core under the Informative References column. We firmly believe that the Framework should not be updated any time soon other than adding ISO/IEC 27001 processes to the Informative References. However, it is our expert opinion that when the Framework is updated, in some years to come, there are several additional areas that such update could address: identifying and categorizing suppliers, overall monitoring and improvement, overall risk monitoring, reducing the risk of counterfeits in ICT components, and flowing security requirements to suppliers and sub-suppliers. These potential updates were identified during the NIST workshop on supply chain risk management on October 1-2, 2015.
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?	Collecting and making available a variety of case studies and sector-implementation approaches for implementing the Framework is useful to the organizations using the Framework. For example, C2M2 is widely used by electric utilities because it helps gauge maturity of security programs along 10 functional domains. Using C2M2 in conjunction with the NIST Framework is detailed in the Energy Sector's NIST Cybersecurity Framework Implementation Guidance. However, such case studies need to be carefully organized and categorized to avoid overwhelming the audience with the content and the detail that is not relevant to them. Including this information in the Framework itself will be counterproductive. The NIST Framework is one of the shortest and most concise sources currently available to guide implementation of cybersecurity programs. If more detail is added to the Framework it will make it more voluminous, detailed, confusing, and less read and used. Continuing the work that NIST has done at http://www.nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm will provide a useful reference library that is modular and specific which is exactly what the audience needs. UTC members appreciate the many and valuable resources available on the program website, however, we would to propose two additional Use Cases for development and publication. One would be a start to finish implementation manual for a small electric utility, as written by and for a power engineer or operations manager with little IT or cybersecurity experience. The guide should include approaches for scoping and estimates for implementation time and cost, as well as a discussion on the cost of ownership once fully implemented. Utility Boards of Directors are extremely cost-conscience and cyber-security projects are notoriously hard to develop meaningful return on investment (ROI) numbers. The second guidance we would like to see is a Use Case for an electric utility who has successfully implemented the framework in a mixed IT and OT environment. In many utilities IT and OT are managed and run by different chains of command. The Use Case would describe how a utility that is structured this way bridges the divide and develops a holistic Framework-based program that addresses the unique characteristics of each (IT and OT) environment.

#	Question Text	Response Text
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?	At this point in time developments made in the nine areas should be used to provide implementation guidance on specific areas of the Framework, rather than integrate yet more information into the Framework. Potential updates beyond the near future are detailed in Question 12.
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	As mentioned above it is premature to update the Framework. Providing implementation guidance and expanding on the references specific to individual categories and subcategories, as described in Question 11, will help organizations implement the Framework while minimizing the impact of any updates.
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?	UTC members appreciate the number and the variety of guidance documents available on the program website.
17	What, if anything, is inhibiting the sharing of best practices?	Individuals charged with protecting utility systems and networks at UTC member organizations are overloaded with work. So are technical management, network engineering and other similar professionals who, while they do not have the word "security" in their title, have security as a part of their responsibilities. There is more need than individuals available and the hours in the day that those who are qualified have. Sharing of best practice requires time commitment and not every organization or every individual is able to afford to break away from their daily work. Limited human bandwidth and availability of expertise is one of the main reasons why best practices are not shared.
18	What steps could the U.S. government take to increase sharing of best practices?	US government could provide on line platforms for sharing, issue grants to industry organizations to facilitate knowledge sharing (different from information sharing), and helping more mature organizations take time to share with less mature. Additionally, NIST could establish a series of regular sharing meetings, in the format of presentations, panels, and workshop sessions where the industry or specific critical infrastructure sectors are able to come together and share what they have done. NIST has done a tremendous job convening the industry and documenting results of discussions. Such meetings would continue this work but also provide outputs for the larger community to use.

#	Question Text	Response Text
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)?	There is an inherent challenge in facilitating sharing through the government sources. However, NIST can work with private organizations to help establish awareness programs for specific constituencies. NIST could then convene regular (semi-annual) Forums/Conferences where such organizations (or any other entities) could share their lessons learned in implementing or otherwise using the Framework to improve security posture. Creating and sharing industry use case studies will provide a structured approach for sharing NIST Framework implementation experience.
20	What should be the private sector's involvement in the future governance of the Framework?	NIST established an effective process for public/private collaboration. Private sector welcomes continued involvement in this process. Private sector is where innovation happens and lessons are learned. Private sector would welcome continued participation in the already established collaborative process.
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	NIST should not transition any portion of the Framework coordination to another organization at this time. The beauty of the process established by NIST is that it does not require any upfront payment (e.g., membership fee) and it welcomes new participants who may or may not be experts in cybersecurity. Transitioning any pieces of the Framework to another organization may result in negative impacts such as limiting access of some private sector organizations to the collaborative process that created the Framework in the first place. We believe that NIST should continue to be the custodian and developer of this Framework for the foreseeable future.
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	See Answer to 21. UTC believes that transitioning any piece of the Framework to another organization is premature and may result in negative consequences.
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?	The reason why we believe that transitioning the Framework is premature is that any organization will require funding to stay in business. Such funding can come from revenue-generating activities, membership dues, or government funding. Revenue-generating activities will distract the organization from its purpose. Membership dues will limit participation and therefore input into subsequent deliverables to better resourced companies and will leave smaller or less resourced organizations behind. With respect to government funding it is unclear why a separate organization (outside of NIST) should exist if its sole source of funding is the US government. NIST staff already has the knowledge and understanding of the Framework and have the support of the security community to continue. We question whether such organization can be self-sustaining and are concerned that transitioning to such organization will have unintended consequences that will distract from or damage Framework implementation activities.

#	Question Text	Response Text
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?	UTC believes that transitioning any piece of the Framework to another organization is premature and may result in negative consequences.
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?	UTC believes that transitioning any piece of the Framework to another organization is premature and may result in negative consequences.