1. Introduction/Our Understanding

Utilities Telecom Council (UTC) is pleased to submit this response to the National Institute of Standards and Technology (NIST) Request for Information in support of the development of the Cybersecurity Framework. UTC believes that developing a risk-based Cybersecurity Framework that can be applied across critical infrastructure sectors is an important effort that will help improve cybersecurity across critical infrastructure. UTC is looking forward to supporting NIST's development of the Framework.

Our response reflects UTC member inputs and a listening tour that we performed over the last 6 months. The listening tour included various UTC member organizations, collectively providing electric power and gas services to over 40 million customers in North America. It was conducted with utilities technology practitioners (cybersecurity, information technology, telecommunications, and control systems personnel) at a variety of organizational levels, including engineers, Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs).

Overall, we believe that a number of useful cybersecurity frameworks already exist that can be generalized, repurposed, and then tailored to specific infrastructure sectors in their own contexts. We would also like to note that electric and nuclear utilities are already subject to North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) and Nuclear Regulatory Commission cybersecurity requirements.

UTC believes that adoption of the Framework should be:

1. Voluntary: facilitated through public/private partnership and other collaborative efforts.
2. Straightforward and written at a high level, so that it can be applied successfully across multiple critical infrastructure sectors.
3. Not prescriptive, as It needs to allow for tailored implementation and for the use of technologies and techniques that are yet to be developed.
4. Tailorable to individual sectors wherever the context requires.
5. Scalable and flexible to ensure that it can be successfully applied to tremendously diverse utilities industry.

1.1 UTC Overview

Founded in 1948, the Utilities Telecom Council (UTC) is a global trade association dedicated to being the source and resource for information and communications technology (ICT) solutions for utilities and other critical infrastructure industries. UTC brings a worldview with regional focus as a market leader for utility telecommunication advocacy and educations with entities in Europe, Canada, Latin America, the Middle East, Asia and Africa. UTC core members include utility (energy, water, gas) pipeline and other critical infrastructure companies that operate mission-critical telecommunications and data networks in support of their core business operations.

1.2 Key Principles

UTC would like to propose a number of key principles for the development of the framework, beginning with its scope. The scope of this initiative should remain limited to critical infrastructure that could be compromised through cyber exploitation and which, if incapacitated, could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. It should address only key assets specifically identified by critical infrastructure owner/operators that, if compromised, could have a material impact on public safety or operational reliability. For the electric and nuclear sectors, the framework should focus narrowly on bulk electric system reliability and should not expand to all digital equipment or cyber assets. Specifically, we are proposing the following principles:

1. **Private sector engagement because it's their business.** Utilities take cyber security very seriously as a part of their overall focus on reliability and resiliency (i.e. "keeping the lights on"). More broadly, the private sector—which owns and operates approximately 85% of the nation's critical infrastructure and maintains unmatched technical and standards-setting expertise—should help develop and subsequently vet the framework.

2. **Cover all sectors, but avoid duplication.** The framework should cover all critical infrastructure sectors while recognizing existing regulation and avoid creating additional or duplicative burdens for highly-regulated industries.

3. **No exemptions.** Current regulations too often place the burden of security on the asset owner; however, the framework should be balanced across asset owners and suppliers to critical infrastructure. Suppliers of critical infrastructure equipment should be required to provide products proven through testing to meet minimum security requirements before being utilized by critical infrastructure sectors.[1]

4. **Utilize existing sector-specific regulatory structure.** The electric and nuclear sectors already have cyber security regulation and standards from both FERC and the NRC. Although other critical infrastructure sectors such as water, gas, pipelines, rail, and telecomm do not have mandatory and enforceable cyber security standards, the electric and nuclear sectors do. Regulatory oversight by other entities would duplicate and potentially undermine strict FERC and NRC oversight.

5. **Leverage existing risk-based, performance-based standards and link compliance.** The framework should be high-level and flexible enough to accommodate and recognize existing standards and standards-development processes. Moreover, compliance with qualified existing standards should translate to compliance with the newly-developed framework. For the electric and nuclear sectors, established processes and existing risk-based, performance-based standards have incorporated input from various stakeholders to ensure that essential systems have been identified and protected; this should satisfy all requirements of the framework.[2]
    - The electric sector has had cyber security standards since 2003 with the adoption "1200" standards adopted by NERC, the FERC-certified electric reliability organization.

[1] Previous compromises of major technology suppliers have created additional cyber security risks for federal agencies and owners/operators of critical infrastructure.

[2] Current standards for the electric and nuclear sectors already cover critical cyber asset identification, security management (including policy and governance), risk assessment and training for personnel, network security, physical security, cyber asset hardening and monitoring, incident response (including mandatory reporting), disaster recovery, configuration management, vulnerability assessments, and protection of sensitive information.

These standards formed the basis of the NERC Critical Infrastructure Protection (CIP) standards that became mandatory and enforceable under FERC's authority in 2006.

- The NRC issued a cybersecurity rule 10 CFR 73.54 in 2009 and accompanying Regulatory Guide in 2010 affecting all nuclear power reactor licensees. The regulation requires licensees to submit a comprehensive cyber security plan and an implementation timeline for NRC approval.

6. **Include only essential systems.** The framework should focus efforts on systems that owners/operators determine to be essential because of their closeness to and understanding of risks associated with the cyber environments in which their systems operate. Any standards governing critical infrastructure companies should regulate only those systems essential to operational reliability or safety as designated by the owner/operator. For the electric and nuclear sectors, these designations already are stipulated in the North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) standards and Nuclear Regulatory Commission (NRC) 10 Code of Federal Regulation (CFR) 73.54.

7. **Consider cost-benefit analysis.** Because the framework cannot eliminate all cyber security risks, preparation and response capabilities are equally important. The framework needs to provide critical infrastructure industries cost recovery opportunities and also consider cost/benefit for the customer. Because prescriptive, cross-sector standards may prove too costly or inefficient, owner/operators need the flexibility to (1) develop customized, layered defenses that prioritize and isolate key assets and/or (2) enhance recovery and response capabilities.

8. **Preserve and build upon existing private-public partnerships.** The framework should encourage enhanced cooperation between government and industry. Department of Homeland Security (DHS) and sector-specific agencies have been working with the private sector for more than a decade to improve information-sharing, operational resiliency, and emergency response capabilities of critical infrastructure industries. For example, DHS in 2009 developed the Private Sector Preparedness program (PS-Prep), which is a voluntary certification program encouraging conformance to consensus-based preparedness standards and best practices. Separately, the electric sector partners with DHS, the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC) to protect infrastructure through the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) which shares threat information with voluntary industry participants.

9. **Provide liability protection for participants.** The framework should offer incentives for voluntary adopters such as liability protection for private sector entities that comply with the framework and cooperate with federal agencies to enhance the security of the nation's critical infrastructure.

1.3 Structure of this Response

UTC has organized this response to provide information related to the questions asked by the NIST Cybersecurity Framework RFI. Each subsequent section provides the specific questions relevant to the section upfront. Not all of the questions are addressed in this response as described in Section 6.

2. Critical Infrastructure Cybersecurity Challenges

This section addresses the following RFI questions (RM stands for Current Risk Management Practices questions in the RFI, FR stands for Use of Frameworks, Standards, Guidelines, and Best Practices):

ID	Question
RM-1	What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?
RM-2	What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?
FR-9	What other outreach efforts would be helpful?

Over the recent past, the utilities sector has made remarkable progress in cybersecurity. Several significant challenges need to be overcome to ensure that this progress continues. During UTC's informal survey, UTC members identified five challenges that applied across the utilities sector and across utility ownership types, including investor-owned utilities (IOU), cooperatives, and municipally-owned utilities. These challenges include:

1. **Information Sharing: UTC believes that a robust legal framework is needed to share threats and vulnerabilities information both among utilities and between utilities and the Federal Government, such as providing appropriate liability protections to the critical infrastructure entities.** We welcome the expansion of the Enhanced Cybersecurity Services (ECS) program and the expedited process for granting clearances for cybersecurity practitioners within critical infrastructure industries, as stated by Executive Order (EO) 13636. While these and other initiatives described in the EO will help the situation, regulatory and legal barriers remain that effectively dis-incentivize utilities from sharing cybersecurity threat and vulnerability information. Currently, utilities hesitate to share cybersecurity threat and vulnerability information with each other and with the government, due to concerns about having to release this information to the general public once it is shared informally; the possibility that the information may be subject to non-disclosure agreements with the vendors and therefore being unable to share product-specific vulnerabilities; and due to the overall reputational risk of acknowledging a cybersecurity issue.

2. **Building Cultural and Community Awareness: UTC believes that efforts to implement the Cybersecurity Framework should include a substantial outreach component that speaks to audiences beyond utility technology practitioners. This outreach should especially include critical infrastructure organizations' boards and executives to facilitate change from the top of the organization.** Utilities have a well-established safety culture that permeates their organizations. They are now working on making cybersecurity a similarly understood property. Outside of utility technology professionals (including those working in information security/information assurance/cybersecurity, information technology [IT], and telecommunications fields), the broader utility community is working on and could use further support expanding awareness of the current cybersecurity threat environment and appropriate processes and techniques that can be applied to reduce cybersecurity risks throughout utility organizations.

3. **Architecture, Infrastructure, and Diverse Cyber Practices: UTC believes that the Cybersecurity Framework should be flexible and scalable to accommodate organizations of different sizes,**

maturity of cybersecurity practices, and diverse IT architectures. IT and network infrastructure and architecture vary greatly among utilities, creating a challenge for generalizing detailed risk management actions. Cybersecurity practices vary widely across different utilities, based on the size of the company and the availability of resources.

4. **Secure Information and Communication Technology (ICT) Products: UTC believes that Cybersecurity Framework should appropriately balance the responsibility for secure ICT in the utilities space between asset owners/operators and their ICT suppliers. This guidance should include establishing and articulating a set of applicable security requirements and an approach for monitoring adherence to these requirements. Conformity assessments provide a useful tool for achieving this objective.** Utilities depend on their ICT vendors to implement a number of cybersecurity controls that could be effective in reducing cybersecurity risks. ICT vendors who have been operating in the general IT space and whose technologies have been subjected to cybersecurity threats originating from the Internet for the past 10-20 years have instituted a number of cybersecurity processes and controls that improved the robustness of those technologies. A number of vendors that have been providing ICT products to the utilities market have not implemented cybersecurity processes and controls with the same uniformity as the IT vendors. While the situation is improving, utilities are currently limited in their risk reduction efforts by the limited availability of products that fulfill both their business needs and their security requirements.

5. **Utility-focused Cybersecurity Workforce: UTC believes that a government-led campaign (similar to the one for general cybersecurity practitioners) is needed, including new educational degrees or concentrations/certificates, incentives for entering careers in the field of utility cybersecurity, and changes to college curricula to increase general awareness among technology professionals.** UTC applauds the US government efforts in establishing National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) as well as the National Initiative for Cybersecurity Education (NICE). These efforts are currently creating the underpinnings of a cybersecurity workforce for the future. Like the current shortage of general cybersecurity experts, there is a shortage of qualified cybersecurity experts that have expertise in utility networks. Utilities are experiencing both a shortage of senior talent that can advocate cybersecurity priorities to company executives, and a shortage of qualified cybersecurity talent that can implement the necessary practices within the operational environment. There are simply not enough qualified cybersecurity professionals who have experience in the utilities sector.

Finally, any development of the Cybersecurity Framework should take into account the practical limits of human ability to absorb information and to act on multiple simultaneous fronts. All of the UTC members we have spoken with were simultaneously pleased by and frustrated with the amount of cybersecurity-related information available for their use and the number of working groups (over 60) currently operating in the utilities cybersecurity space. While the information and the working groups are extremely useful, the current workforce shortage results in these individuals' inability to study all of the available material and participate in all the groups. Great quantities of information and resources are not being used because of information overload. Prioritizing the framework will be critical to its success.

3. Utilities Cybersecurity Summary

This section addresses the following RFI questions (RM stands for Current Risk Management Practices questions in the RFI):

ID	Question
RM-3	Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?
RM-4	Where do organizations locate their cybersecurity risk management program/office?
RM-5	How do organizations define and assess risk generally and cybersecurity risk specifically?
RM-6	To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

A number of UTC members have initiated collaborative interaction to discuss cybersecurity among the technology professionals within their organizations. This has occurred regardless of the governance, organizational design, and reporting structure. This interaction ranges from semi-annual meetings to monthly meetings and, in the most frequent cases, includes management-level and practitioner-level interaction. This interaction ensures that cybersecurity is addressed by the involved utility technology practitioners, including IT/cybersecurity, operations, and telecommunications.

There is no single prevalent governance structure for cybersecurity among UTC members. Among those we visited, the organizational placement of utilities technology practitioners that have an impact on cybersecurity (IT/cybersecurity, operations, and telecommunications) varied. One utility had all three technology practitioner types reporting to the Chief Information Officer (CIO). Some utilities had three different departments in charge of these three different technology functions. Some utilities had a hybrid model where, for example, telecommunications and IT/cybersecurity were reporting to the same executive, while operations reported to a different executive. We also noticed that the role of Chief Information Security Officer (CISO) did not exist in every utility we visited. Most of the larger utilities had a CISO or a Director of IT/Risk/Security (or a similarly worded position) that in effect was performing the role of the CISO. In those utilities that had designated CISOs, the CISOs reported to the CIOs.

4. Cybersecurity Frameworks

This section addresses the following RFI questions (RM stands for Current Risk Management Practices, FR stands for Use of Frameworks, Standards, Guidelines, and Best Practices) at a high level:

ID	Question
RM-7	What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?
RM-8	What are the current regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?
RM-10	What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?
RM-11	If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?
RM-12	What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?
FR-1	What additional approaches already exist?
FR-2	Which of these approaches apply across sectors?
FR-3	Which organizations use these approaches?
FR-4	What, if any, are the limitations of using such approaches?
FR-5	What, if any, modifications could make these approaches more useful?
FR-6	How do these approaches take into account sector-specific needs?
FR-7	When using an existing framework, should there be a related sector-specific standards development process or voluntary program?
FR-8	What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

The cybersecurity community has produced a rich variety of general and critical infrastructure-specific cybersecurity frameworks. Most of them contain common elements, including a continuous improvement process that consists of a risk assessment, determination of risk treatments and control selection and tailoring, implementation of controls, monitoring of controls, and improvement based on monitoring. These frameworks also provide security control catalogs of a variety of levels of detail. The NIST suite of standards and guidelines and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000, *Information Security Management System*, frameworks are two examples of such frameworks that can be applied across all critical infrastructure sectors. Other frameworks specific to the utilities industry, such as NIST Interagency Report (IR) 7628, *Guidelines for Smart Grid Cybersecurity*, Energy Sector Cybersecurity Capability Maturity Model (ES-C2M2), and IEC 62443/Industrial Society for Automation (ISA) 99 series of standards for industrial automation and control system security are either based on NIST or ISO frameworks or are harmonized with them. Subsequent sections provide further information on these linkages among generic and industry-specific frameworks.

Additionally, some frameworks do not provide a process for conducting a risk assessment because the authors have already conducted a general risks assessment and created a resulting control set based on that risk assessment. The Top 20 Critical Controls[3] are an example of a framework that assumes a completed risk assessment and recommends controls based on that risk assessment.

[3] http://www.sans.org/critical-security-controls/guidelines.php

4.1 General Cybersecurity Frameworks

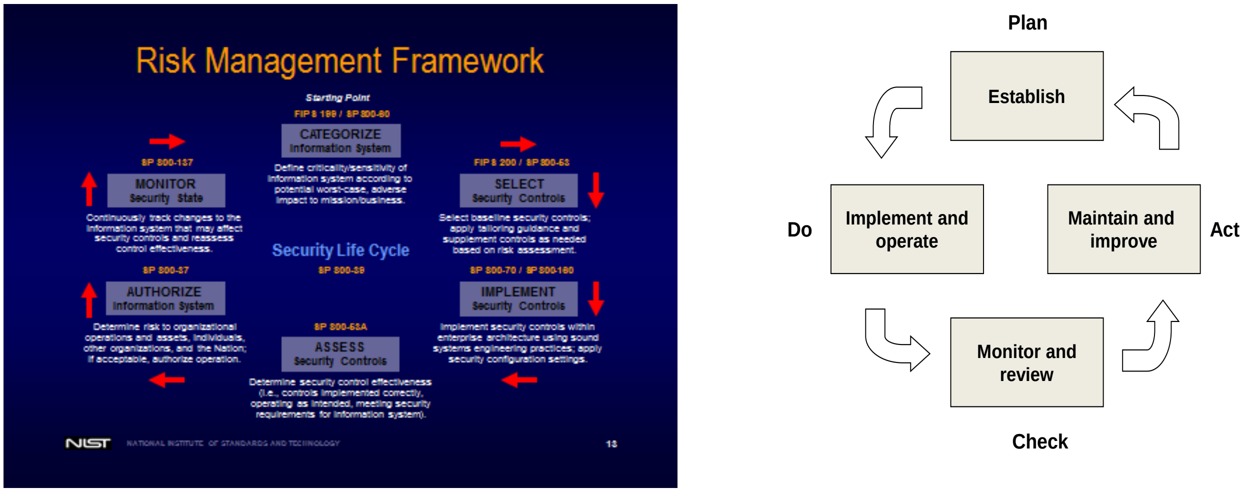
Many UTC members use NIST and ISO frameworks as the basis for their controls catalog (NIST Special Publication [SP] 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*[4], and ISO/IEC 27002, *Code of Practice for Information Security Management*) and for their enterprise cybersecurity risk management framework (ISO/IEC 27001, *Information Security Management System Requirements*) to determine what processes and controls to implement. Utilities use NIST and ISO frameworks as best practices because they are not required to implement them.

4.1.1 Frameworks Overview and Comparison

Each of the two frameworks provides processes that include risk assessment, controls selection, controls implementation, controls and process monitoring and improvement. The controls catalogs within these frameworks are at differing levels of detail due to the different audience that these frameworks target:

- NIST SP 800-53 controls are detailed and specific because they originated from a system-based approach where controls are applied to specific systems
- ISO/IEC 27002 controls are high level and are meant to remain at the "management" level because they originated from an enterprise-based approach where it is up to the enterprise to determine how to implement the controls.

The NIST Risk Management Framework, depicted in Figure 1, coupled with the overall Risk Management Process and Risk Management Hierarchy, described in NIST SP 800-39 provide the overall "Framework" for cybersecurity that can be generalized and then adopted for the critical infrastructure. Also depicted in Figure 1 is ISO/IEC 27001, Information Security Management System that provides a similar framework but with less detail, due to the need for an ISO standard to be scalable to different organizational sizes and applicable across the globe in multiple legal and regulatory regimes.



Risk Management Framework

Starting Point
FIPS 199 / SP 800-60
CATEGORIZE
Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200 / SP 800-53
SELECT
Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70 / SP 800-160
IMPLEMENT
Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A
ASSESS
Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-37
AUTHORIZE
Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-137
MONITOR
Security State
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle
SP 800-39

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 13

Figure 1. NIST Risk Management Framework and ISO/IEC 27001 Framework

[4] UTC members use prior versions of NIST SP 800-53 but are likely to transition to the new controls catalog in the future.

ISO/IEC 27001 framework steps are:

- Plan (establish the ISMS) – Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- Do (implement and operate the ISMS) – Implement and operate the ISMS policy, controls, processes and procedures.
- Check (monitor and review the ISMS) – Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- Act (maintain and improve the ISMS) – Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.[5]

NIST and ISO frameworks were developed and codified over the last 10-15 years. Both frameworks are augmented by numerous other standards that provide guidance on how to implement the processes and the controls described in the frameworks. The following are some examples of such documents:

- Conduct a risk assessment for each of the frameworks – NIST SP 800-30, *Guide for Conducting*
- *Risk Assessments,* and ISO/IEC 27005, *Information Security Risk Management*
- Measure effectiveness of processes and controls for each of the frameworks – NIST SP 800-55, *Performance Measurement Guide for Information Security,* and ISO/IEC 27004, *Information Security Management – Measurement*
- Implement individual controls for each of the frameworks – NIST SPs about access controls and ISO/IEC standards on network security, applications security, etc.

The ISO/IEC suite of information security standards also includes a substantial number of standards addressing identity management and privacy techniques.[6]

4.1.2 Limitations and Potential Modifications

NIST and ISO frameworks are inherently high level because they have to apply to a broad set of organizations. NIST standards and guidelines have to provide guidance at the right level to apply to the entire Federal agency community, in some cases including Department of Defense and the Intelligence Community. ISO/IEC standards have to provide guidance at the right level to apply globally, to large and small organizations, multiple industries, and a variety of legal and regulatory regimes.

However, the fact that these frameworks are high-level enables them to be adjusted to various contexts, including sector-specific contexts. Within the frameworks themselves, the risk assessment process provides for selecting only relevant controls. The ISO framework goes further in explicitly allowing deviation from the ISO controls catalog and development or tailoring of non-ISO controls to sector-specific sector needs, as long as this deviation is explained and documented.

[5] ISO/IEC 27001, Information Security Management System – Requirements

[6] ISO/IEC standards that address cybersecurity and privacy techniques can be found at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306&development=on. Most of these standards are applicable cross-sector and are not specific to any one sector.

However, any modifications to provide greater detail in either framework will be counterproductive for a variety of reasons, including but not limited to:

- Being impractical for an organization that uses more advanced techniques that are not prescribed by the framework and therefore stifle innovation and improvement of cybersecurity, e.g., if the framework specifies the use of manual testing and omits the use of automated testing, this may restrict more advanced automated testing.
- Excluding organizations that implement practices differently but achieve the same results, e.g., if the framework requires annual training of users and omits daily user updates in place of annual training, this may restrict a more effective method of training.
- Excluding sectors that for operational reasons cannot apply certain controls, e.g., utilities find acquiring certain types of telecommunications equipment that provides for individual user authentication a challenge due to the existence of few available solutions with that feature set. If the framework does not provide for exceptions use of this technology, the organization will be non-compliant with the framework.

UTC believes that the Cybersecurity Framework should remain general and not prescriptive to allow for the different size, scale, and maturity of user organizations.

4.1.3 Sector-Specific Use of NIST and ISO Frameworks

Both NIST and ISO approaches already provide for the adaptation and tailoring of the control sets to sector-specific needs:

- NIST SP 800-53 Rev4 introduces a concept of overlays that can be used to adapt the NIST control set to the sector-specific context.
- ISO/IEC 27001 allows for use of a variety of control sets as long as that decision is documented. Furthermore, the committee that develops the ISO/IEC 27001 standard and other standards that support ISO/IEC 27001 has a process for creating sector-specific controls that has been implemented in ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.* This process is also currently being implemented to develop ISO/IEC 27017, *Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002.*

UTC believes that both frameworks can be used to address sector-specific needs by creating extensions of generic controls catalogs to address sector-specific needs and provide more detailed and applicable guidance that can be implemented within individual sector environments.

4.2 Sector-Specific Cybersecurity Frameworks

UTC members use several sector-specific frameworks to augment the general information security frameworks described in Section 3.1, including:

- NERC CIP which some of the utilities are required to implement
- NIST 7628
- ES-C2M2
- IEC 62443/ISA99.

4.2.1 NERC CIP

Utilities are subject to mandatory cybersecurity requirements that apply to the bulk electric system, which includes all facilities operated at or above 100 kV.[7] These requirements are developed and adopted through the North American Electric Reliability Corporation (NERC). The NERC critical infrastructure protection (CIP) standards have been in place for years, but were made mandatory in accordance with the provisions of the Energy Policy Act of 2005 (EPACT 2005). Under these provisions, FERC is authorized to review and adopt the CIP standards that are adopted by NERC.[8] FERC does not have authority to develop cybersecurity standards itself; it may only approve or reject the standards that are developed by NERC. Utility compliance with the mandatory NERC CIP standards is audited by NERC auditors, and utilities are subject to fines and penalties of up to $1 million per day/per violation.

The NERC CIP standards have gone through several versions of development. The initial CIP standards were approved in part by FERC in 2008.[9] In approving the initial CIP standards, FERC directed NERC to implement additional recommendations by FERC to improve the standards. NERC has been working towards implementing the remaining recommendations under FERC Order 706, culminating in the most recent version of NERC CIP. NERC CIP version 5 implements all of the remaining recommendations by FERC in FERC Order 706.

The current status of NERC CIP is that version 4 has been adopted by FERC,[10] and version 5 has been approved by NERC and has been submitted to FERC for approval.[11] NERC CIP version 4 are scheduled to take effect on April 1, 2014, but may be superseded by NERC CIP version 5 if it is adopted by FERC before version 4 goes into effect.[12] NERC CIP version 5 builds on the brightline standards of version 4 by categorizing cyber assets that represent a high, medium or low risk to the bulk electric system (BES), thus providing utilities the flexibility to apply cyber security requirements appropriately according to the risk to the BES.[13] Hence, "the intent is to change the basis of a violation in those Requirements so that

[7] Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure, Final Rule, Docket Nos. RM12-6-000 and RM12-7-000; Order No. 773, 141 FERC ¶ 61,236, http://www.ferc.gov/whats-new/comm-meet/2012/122012/E-5.pdf.

[8] NERC was appointed as the Electric Reliability Organization (ERO) by FERC, under the provisions of the EPACT 2005, which directs the FERC to appoint the ISO to develop and adopt the reliability standards.

[9] Mandatory Reliability Standards for Critical Infrastructure Protection, Docket No. RM06-22-000, Order No. 760, 122 FERC P 61040 (2008).

[10] Version 4 Critical Infrastructure Protection Standards, Docket No. RM11-11-000, Order No. 761, 139 FERC P. 61058 at ¶¶79, 110-111 (2012).

[11] http://www.nerc.com/files/Final_Petition_CIP_V5_01-31-13%20and%20Exhibits%20A-E.pdf

[12] Note that the Version 5 Implementation Plan states that version 5 will replace version 4 once version 5 goes to effect. *See* Implementation Plan for Version 5 CIP Cybersecurity Standards at 2, *visited at* http://www.nerc.com/docs/standards/sar/Implementation_Plan_clean_4_%282012-1024-1352%29.pdf

[13] The new definition of BES cyber assets 1) enables for the grouping of critical cyber assets together such that the system may be protected as a whole instead of requiring each component to comply; and 2) provides a convenient level at which a Responsible Entity (RE) can organize their documented implementation of the requirements and compliance evidence. CIP version 5 leaves it up to the Responsible Entity to determine the appropriate level of granularity when determining a particular BES cyber system. "Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess." CIP-002-5 — Cyber Security — BES Cyber System Categorization at 5, visited at http://www.nerc.com/files/CIP-002-5.pdf.

they are not focused on whether there is a deficiency, but on identifying, assessing, and correcting deficiencies."[14]

4.2.2 NISTIR 7628

NISTIR 7628 is an important best practice document that applies to smart grid. Many UTC members use it to inform their smart grid implementation and have provided positive feedback about its impact. NISTIR 7628 draws extensively on other NIST standards and guidelines including NIST SP 800-53. Specifically, it provides a controls catalog based on NIST SP 800-53.

4.2.3 ES-C2M2

ES-C2M2 is an important framework that was developed by a public-private partnership led by the Department of Energy. Many UTC members use ES-C2M2 for internal process assessments and have provided positive feedback about its impact.

ES-C2M2 lists seven foundational resources, two of which are NIST IR 7628 and Carnegie Mellon Computer Emergency Response Team (CERT) Resilience Management Model (RMM). NISTIR 7628 includes a controls catalog for smart grid security based on NIST SP 800-53. CERT RMM is based on a number of frameworks, including NIST and ISO/IEC 27000 frameworks. Much of the ES-C2M2 origin is to a large extent in NIST and ISO cybersecurity framework.

4.2.4 IEC 62443/ISA99

The IEC 62443 series focuses on Industrial Control Systems security. Many UTC members use these standards. These standards are developed by ISA99 committee and are then adopted by IEC Technical Committee (TC) 65. As far as harmonization with the general cybersecurity frameworks, IEC TC65 has a liaison relationship with ISO/IEC JTC1 SC27 that is chartered with the development of general information security standards and is responsible for ISO/IEC 27000 framework and supporting standards. IEC 62443-2-1 (Security Management System) is currently in the process of being harmonized with ISO/IEC 27001.

4.3 Conformity Assessments and Standards Development Organizations

Conformity assessment is an important mechanism that helps demonstrate that specified requirements for a product, process, or system are fulfilled. Conformity assessments can help critical infrastructure organizations ascertain that:

- They have actually implemented the security requirements that they set out to implement and identify areas for improvement
- Their suppliers have implemented security requirements that have been articulated.

Standards Development Organizations (SDO) play an important role in developing consensus-based standards and guidelines. International SDOs also play an important role in providing consensus-based conformance assessment frameworks that are applicable globally. Critical infrastructure organizations and ICT vendors can use international conformity assessment approaches to negotiate and articulate security requirements and to monitor fulfillment of these requirements. Internationally-developed and globally-used conformity assessment approaches facilitate improvement in the cybersecurity posture of the global ICT and critical infrastructure which benefits national US interests.

[14] *Id.*

Of the frameworks discussed above, ISO/IEC 27001 conformance can be certified through a conformity assessment process. IEC TC65 is in the process of developing requirements for control systems suppliers in IEC 62443-2-4.

4.4 Performance Measurement

Utilities are focused on providing reliable service in a safe manner. Reliability and safety are primary goals in the utilities space. In practice, tying cybersecurity indicators to these overall goals has proven challenging. While the challenge is real, a number of standards, guidelines, reports, and research efforts have emerged over the last 15 years that provide guidance on how to establish a cybersecurity measurement program. These guidelines, including NIST and ISO documents mentioned in Section 4, agree on a basic process for the development of cybersecurity measures, which is, while conceptually simple, challenging to execute.

Cybersecurity metrics/measures must be based on business or mission goals and objectives. Without being tied to the mission context of the organization it is challenging to make these metrics meaningful to provide actionable data for executive decision making. As the Cybersecurity Framework is developed and implemented, the first types of measures that will be available and feasible to collect will be those that will address the degree to which the Framework is implemented (NIST SP 800-55 calls these *implementation measures*). While these measures will not demonstrate whether the infrastructure is more effective because the Framework is implemented, they are necessary and cannot be bypassed to determine whether the Framework is effective in improving cybersecurity of the national critical infrastructure (NIST SP 800-55 calls these *effectiveness/efficiency measures*). Determining whether the Framework has accomplished its objective of improving cybersecurity of critical infrastructure will take time and will require substantial pieces and parts of the framework to be implemented, at least within some organizations. Determining impact (NIST SP 800-55 calls these *impact measures* while other measurement frameworks call these *outcome* measures) will also take time. Both efficiency/effectiveness and impact measures will require that the data about the results of Framework implementation to be available, normalized, and tied to the overall objectives of the Framework.[15]

UTC believes that is critical that the cybersecurity community manages its collective expectations with regards to implementing cybersecurity performance measures. Outreach efforts may be required to educate the community on the basics of cybersecurity measurement, including the natural maturing and progression that is required to gain the maximum benefit.

4.5 Regulatory Reporting

Utilities are subject to national, as well as state and local reporting requirements and guidelines related to cybersecurity. These include NERC CIP-008 (Incident Reporting and Response Planning) requirements;[16] Department of Energy (Emergency Incident and Disturbance Report) requirements; and

[15] In addition to NIST SP 800-55 Rev1 and ISO/IEC 27004, the following two documents provide information on security measurement process framework/model and maturity of security measurement, respectively: DHS, *Draft Practical Measurement Framework for Software Assurance and Information Security,* https://buildsecurityin.us-cert.gov/swa/downloads/SwA_Measurement.pdf; Lippmann et al, *Continuous Security Metrics for Prevalent Network Threats: Introduction and First Four Metrics* http://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2012_05_22_Lippmann_TechReport_FP.pdf

[16] *See e.g.* NERC CIP 008-5, available at http://www.nerc.com/files/CIP-008-5.pdf. Note that this version has been adopted by NERC, but has not been approved yet by FERC. NERC CIP 008-4 has been approved by FERC and is

state public utility commission reporting requirements,[17] as well as voluntary disclosure guidelines by the Securities and Exchange Commission[18]; the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[19] and NERC's Energy Sector Information Sharing Analysis Center (ES-ISAC)[20].

For example, NERC CIP-008 specifically requires utilities to develop and maintain a Cyber Security Incident Response Plan, which must address at a minimum

1) Procedures to characterize and classify events as reportable Cyber Security Incidents.
2) Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.
3) Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.
4) Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
5) Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.
6) Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

In addition, NERC CIP-008 requires utilities to provide relevant cybersecurity incident documentation related to cybersecurity Incidents for three calendar years.

Another example is the mandatory standards for nuclear power reactor licensees, 10 CFR § 73.54 "Protection of digital computer and communication systems and networks" for nuclear power plants, by the Atomic Energy Act and the Nuclear Regulatory Commission (NRC). This regulation requires licensees to submit a comprehensive cybersecurity plan and an implementation timeline for NRC approval.

scheduled to go into effect in April 2014. *See* NERC CIP 008-4 available at http://www.nerc.com/files/CIP-008-4.pdf

[17] *See e.g.* Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission (Sept. 2012), available at http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf; Report on Electric Grid Cybersecurity in Texas (Nov. 2012), available at http://www.google.com/url?sa=t&rct=j&q=utilities%20are%20required%20to%20report%20cybersecurity%20incidents%20within&source=web&cd=57&cad=rja&ved=0CFMQFjAGODI&url=http%3A%2F%2Fwww.puc.texas.gov%2Findustry%2Fprojects%2Felectric%2F40128%2FPUCT_Project_40128_Electric_Grid_Cybersecurity_in_Texas.pdf&ei=h2JdUczLAYyC8QSB24D4Dg&usg=AFQjCNHTtT67mqlyH1_1nWpBv16DK4HdaQ; *and* Cybersecurity for State Regulators With Sample Questions for Regulators to Ask Utilities, NARUC (June 2012), available at http://energy.gov/sites/prod/files/NARUC%20Cybersecurity%20for%20State%20Regulators%20Primer%20-%20June%202012.pdf

[18] *See* SEC CF Disclosure Guidance: Topic 2, available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[19] *See e.g.* ICS CERT incident reporting system at https://forms.us-cert.gov/report/

[20] *See e.g.*NERC, Security Guideline for the Electricity Sector: Threat and Incident Reporting, *available at* http://www.nerc.com/files/Incident-Reporting.pdf

A number of other reporting requirements exist, including:

- Securities and Exchange Commission (SEC) requirement to report material information about cybersecurity as it relates to investor interests
- Federal Trade Commission (FTC) requirement to report to customers when certain financial information is compromised as a result of a cyber situation
- State utility regulatory commissions may seek justifications for the recovery of costs incurred to institute cybersecurity measures and may seek information about relevant events
- DOE collects information about outages, including those related to cybersecurity
- Many states require reporting to affected individuals when a cyber intrusion potentially compromises the privacy of individual confidential financial or other information.

4.6 Sector-Specific Agencies and Coordinating Councils

Sector-Specific Agencies (SSA) and related coordinating councils have an important role in providing a collaborative platform for public-private partnership to improve the cybersecurity of the national infrastructure. As the Cybersecurity Framework matures, the SSAs and coordinating councils will be vitally important to serve as a gathering point for industry input and outreach points for engaging the industry in an active dialog. This dialog will help ensure that the Framework addresses industry concerns while facilitating improvement of the national cybersecurity posture.

5. Special Utility Telecom Considerations

This section will address the following question:

ID	Question
RM-9	What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Utilities have designed, built and operated private communications networks for mission-critical applications to support unique operational requirements such as the utilities' need to maintain high reliability and availability of communications service to key utility components and personnel. These are especially critical and relevant during disasters.[21] Utility telecommunications practitioners are responsible for securing these networks which provide services to the operational and business networks, as well as connectivity to the outside world and remote vendor connectivity. Until this infrastructure is secured, securing the services that ride on top of it will be challenging. These challenges will become further exacerbated as utilities are transitioning to smart networks which are entirely Internet Protocol (IP)-based and involve exponentially increasing the number of connected devices.

UTC believes that utilities telecommunications engineers need to be at the table during critical infrastructure cybersecurity-related discussions. They also need to be provided the tools that they require, including sufficient radio spectrum. This section summarizes relevant challenges and their relevance to the development and the objectives of the Cybersecurity Framework.

5.1 Security of the Underlying Communications Network

In addressing the security of IT networks, the Framework should recognize that IT security fundamentally relies on the security and integrity of the underlying physical communications network. It does little good to secure the IT network, if the underlying communications network is vulnerable to outages, congestion and other performance issues.

Utilities and other critical infrastructure entities depend on a robust communications network to provide safe and reliable services that support essential electric, gas and water services to the public at large. That is why for decades, utilities have designed, built and operated their own private internal communications networks, which include wired and wireless communications.

5.1.1 Need for Spectrum

Wireless communications networks depend on access to suitable spectrum to provide capacity and coverage for reliable and cost-effective communications. At this point in time, there is no dedicated licensed spectrum for utility or other critical infrastructure entities' communications networks. Most of the utilities' wireless networks rely on narrowband spectrum which is shared with many other radio operations, such as taxicabs, which may lead to congestion and interference with utility

[21] For specifics on utility communications requirements, see DOE report on Communications Requirements of Smart Grid Technologies, October 5, 2010 (**http://www.smartgrid.gov/sites/default/files/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf**)

communications. Thus, there is insufficient spectrum to meet current needs for wide-area coverage and there is a serious deficit of spectrum to meet future demand associated with the expansion of wireless smart networks and other applications of technology innovation.

UTC believes that as part of the Cybersecurity Framework, relevant SSAs and the Federal Communication Commission (FCC) should address the lack of suitable spectrum needed to support the private internal communications networks of utility and other critical infrastructure industries. These efforts should be conducted in close collaboration with utilities and other critical infrastructure industries, so that the government agencies understand the performance requirements of the networks and be able to work with industry to identify spectrum that would be capable of supporting those performance requirements. Moreover, this effort should be conducted and completed on an expedited basis in order to meet the current and future spectrum needs of utilities and other critical infrastructure industries in a timely manner.

5.1.2 Need to Avoid Interdependencies

While utilities use some commercial communications services, they rely on their own private internal communications networks to support their mission critical applications, particularly during storms, hurricanes and other natural disasters. The role of private networks has been noted in government reports. In a January 2006 report, the Telecommunications and Electric Power Interdependency Task Force (TEPITF) of the President's National Security Telecommunications Advisory Council (NSTAC) observed that electric power service providers largely rely on private, internal communications systems for "mission-critical functions, such as process control systems, supervisory control and data acquisition (SCADA) systems, generation facilities, transmission grids, and the distribution network, including emergency response communications."[22]

Interdependencies between the electric and commercial communications sectors impact national security and emergency preparedness. NSTAC, within the National Communications System (NCS) of the Department of Homeland Security, has stated that, "The inherent interconnection and resulting interdependencies between domestic communications networks and various other infrastructure sectors pose significant threats not only to our national security, but also to the availability of NS/EP communications services and the operational capabilities of other infrastructures reliant upon communications services."[23] The implications for such interdependencies were further explored in a February 17, 2009, report by the Communications Dependency on Electric Power (CDEP) Working Group of the NCS Committee of Principals, which found that because of these interdependencies, long-term outages of electric power could have devastating consequences to millions of people.[24]

UTC believes that national security concerns would seem to demand that interdependency between the electric and communications sectors to be minimized, not increased through misaligned spectrum allocation policies The lack of sufficient spectrum for utility private networks is exacerbating that

[22] NSTAC Report to the President on Telecommunications and Electric Power Interdependencies: People and Processes: Current State of Telecommunications and Electric Power Interdependencies, January 31, 2006, at 3-1 and 3.2. The Report is reprinted in the following compilation of NSTAC reports: http://www.ncs.gov/nstac/reports/2006/NSTAC_XXIX_Reports_082206.pdf

[23] NSTAC, "Addressing Critical Infrastructure Interdependencies and Independence." (http://www.ncs.gov/nstac/nstac_t5.html)

[24] Communications Dependency on Electric Power Working Group Report, "Long-Term Outage Study" National Communications System Committee of Principals, February 17, 2009 (FOUO).

interdependency, because it will have the indirect effect of making utilities more dependent on commercial networks to meet their communications needs. Preservation of both private as well as commercial communications systems should be a priority so that the incapacitation of the commercial wireless system does not lead to incapacitation of electricity and water services.

5.2 Inclusion of Telecommunications Practitioners in the Process

Utilities' physical and information infrastructures evolved organically, resulting in a variety of organizational units and professionals being responsible for portions of such infrastructures, including securing the infrastructures. This evolution began from isolated business and operational systems with telecommunications departments providing network services for both via wired or wireless communications. With the advent of Internet Protocol (IP) technology, utilities deployed IP- based network equipment to manage these networks, which increasingly resulted in convergence of technology used for the overall utility network infrastructure. The business need to provide data from the operational network to the business network, as well as to allow remote vendor connectivity into the utility networks further blurred the strict segregation between the operational, business, and telecom systems and practitioners.

Many industry efforts to date, including standards and guidelines development efforts, include operational and IT/cyberecurity utilities practitioners but not the telecommunications practitioners. This is counterproductive because telecommunications practitioners are vital participants in securing utilities networks, on par with the IT/cybersecurity and operations practitioners.

UTC believes that any the Cybersecurity Framework variant that is tailored to the utilities sector must account for this cross-functional collaborative management of cybersecurity in the utilities space. Any efforts to facilitate adoption of the Framework should explicitly include utilities telecommunications practitioners who will have a vital role in implementing the Framework.

6. Not included in the response

UTC response does not address the questions in the Specific Industry Practices area of the RFI because those are at a detailed operational level. Generally speaking, utilities deploy these practices and augment them with other practices based on the frameworks that they use (NIST or ISO) and on the applicable risk assessment.