Comments template for Preliminary
Cybersecurity Framework

Submitted by:______________________
Date: ______________________

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	AWWA	Kevin Morley	G	1-2	88-104	1.0	In 2008, AWWA collaborated with DHS to develop the *Roadmap for Security Control Systems in the Water Sector* <www.awwa.org/Portals/0/files/legreg/Security/SecurityRoadmap.pdf>. This resource identified a need for actionable guidance to support executive level support for implementing best practices and standards. To fill this void, AWWA took steps in late 2012 to initiate the development of a cybersecurity resource that organized the various standards, practices and controls into actionable steps a utility can take to mitigate the risks of the cyber security threat. This has resulted in guidance and a use-case tool that provide managers with clear direction on how to evaluate their cybersecurity needs and elevate awareness of various best practices and controls. The development of this water sector based cybersecurity resource addresses the gap identified in the 2008 *Roadmap*; expands on existing sector requirements for cybersecurity in *ANSI/AWWA 430: Security Practices for Operations and Management*, which has SAFETY Act designation; supports the priorities in the 2013 *Roadmap to a Secure & Resilient Water Sector,* a CIPAC report of the WSCC/GCC*;* and complements the objectives of EO 13636 and the draft Framework.	The EO and the draft Framework state that sector-specific approach's are to be leveraged and complemented by the Framework. We believe that the approach developed by AWWA, with significant input and direction from water utility owner/operators, subject matter experts, technology providers and state/federal partners, should be recognized and acknowledged as the means by which the water sector will fulfill the principles of EO 13636.
2	AWWA	Kevin Morley	T	3	159-183	1.2	This section is confusing in its application of terms like risk management and risk-based. Line 174-179 offers some guidance to very specific methods of cyber risk management, but because of the narrow application of those reference, they may translate well to the overall organizations risk management strategy due to scope limitations. The purpose of the EO and the framework should be to elevate the priority of the cyber risk at the management level, which call for a more general discussion of how the Framework could be supportive of enterprise risk management. For example, *ANSI/AWWA J100: Risk and Resilience Management for Water & Wastewater Systems,* provides a methodology that includes cyber threats as part of a comprehensive all-hazards risk and resilience analysis.	Strike 1.2 and replace with more general statement of need to incorporate cyber threats into organization risk management strategy. Section 2.2 provides more appropriate conceptual discussion of how the Framework may support consideration of cyber threats. More specifically, section 3.2 offers a more actionable discussion of the process. We believe these principle are well supported by existing water sector standards, *ANSI/AWWA 430 and J100,* both of which have received SAFETY Act designation.

Type: E - Editorial, G - General T - Technical

3	AWWA	Kevin Morley	T	5-6	206-237	2.1	The Framework Core provides an informative organizational baseline, however it is relatively abstract for purposes of enabling asset owners to directly gravitate to the underlying actions that this Framework seeks highlight for implementation. NIST should recognize that many critical infrastructure owner/operators may not have the in-house technical expertise to operationalize some of the controls and practices associated with each Core Function. To make this issue more transactional and therefore accessible, AWWA, on behalf of the water sector, applied a different approach based on direct input from water systems of all sizes. This resulted in a use-case model, where by the asset owner selects a process control system use type, such as "remote system access with control". This generates a series of prioritized controls and practices that the asset owner can apply to enhance security of their operations. This use-case approach "demystifies" cybersecurity by reorienting the asset owners to ways in which they apply various technologies in their operations. In addition, the prioritization step provides the asset owner with an action plan for implementation, especially with limited budget, and/or evaluation of their current cybersecurity status.	AWWA has mapped the controls and practices in the preliminary NIST Framework. While following a slightly different path, we believe the guidance and use-case tool achieve the same objectives by contextualizing them from the perspective of a water utility owner/operator. We encourage NIST to be flexible in their recognition that one-size does not fit all, and support sector specific models as implied in the EO and NIST Framework. The approach AWWA applied results in very directed output regarding recommended practices/controls, that allows for both planning future applications and/or upgrading existing systems as appropriate.
4	AWWA	Kevin Morley	T	7	282-296	2.2	The guidance that AWWA has developed can assist a utility in making this type of classification. However, we find this task to be a unnecessary exercise that distracts the intended audiences focus from the actual recommended practices and controls that will support a more robust and resilient cyber secured infrastructure.	See prior discussion regarding Section 2.1.
5	AWWA	Kevin Morley	T	9-11	321-389	2.4	We believe that the framework implementation tiers process is a distraction to primary objective. Section 2.4 should be modified to describe only the characteristics of a desired end state for a cybersecurity program, such as Tier 4. Organizations should determine a prioritized list of actions to reduce cybersecurity risk through a risk assessment, as described in Section 3.2. Imposing the selection of an implementation tier into this process is a confusing and unnecessary hurdle. Further, no organization will want to assign a low tier to its efforts.	Strike the concept of selecting an implementation Tier in Section 2.4, and replace it with a simple description of the desired characteristics for a robust cybersecurity program, such as Tier 4.

6	AWWA	Kevin Morley	T	11-12		3.2	We agree with the basic steps outlined in this section, exception being step 4 as noted previously. They align very well with the process and methods we have specified in our standards that address security, risk and resilience management, and prepardeness: *ANSI/AWWA G430: Security Practices for Operations and Management*, *ANSI/AWWA J100: Risk & Resilience Management of Water and Wastewater Systems*, and *ANSI/AWWA G440: Emergency Preparedness Practice*s. These steps are also supported by the cybersecurity that we have prepared to support the needs of the water sector.	NIST should consider pulling this section forward to provide readers/public better sense of the process and what they are being asked to do. This process is then supported by the descriptions in section 2.
7	AWWA	Kevin Morley	G			All	The comments submitted by the USEPA are appropriate and we encourage your full consideration of their merit.	