PASADENA WATER AND POWER

April 8, 2013

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

**RE: NIST Docket No. 130208119-3119-01**
**Comments of the City of Pasadena Water and Power in Response to NIST Request for Information on: "Developing a Framework to Improve Critical Infrastructure Cybersecurity."**

Dear Ms. Honeycutt:

Pasadena Water and Power (PWP) is serious about cyber security. The reliability of the grid is of primary importance to us, and to our customers. The electricity sector is likely the most capital-intensive of all infrastructure industries. The survival of our business depends on our ability to protect our investments. We believe that we are performing well, but as in any security effort, continuous improvement is necessary and our efforts depend on the information we receive, the guidance we are given, and the performance of our vendors. PWP hereby respectfully submits these comments in response to the notice and request for information ("RFI") on "Developing a Framework to Improve Critical Infrastructure Cybersecurity," issued on February 26, 2013 by the National Institute of Standards and Technology ("NIST").

As an industry, we have already spent 7 years and significant resources establishing and complying with the Federal Energy Regulatory Commission (FERC) - North American Electric Reliability Corporation (NERC) regime's consensus-based, FERC-approved standards. These standards are developed by electric industry experts addressing all electric reliability concerns, not just cyber security. In fact, the electric and nuclear sectors are the only critical infrastructure sectors with mandatory and enforceable standards in place to address both cyber- and physical-security. These standards are enforceable with financial penalties up to $1 million per day, per violation.

PWP welcomes the President's Executive Order (EO) directive to the Secretary of Homeland Security and the Attorney General to establish a process providing for the rapid dissemination of unclassified and classified information relevant to cyber vulnerabilities, along with information available under the Cybersecurity Services program, to critical infrastructure entities. Establishing strong information sharing practices between federal government agencies charged with ensuring domestic security, the intelligence community and industry is essential in protecting critical assets from intrusion and disruption. To date much of this information has been shielded from entities seeking to manage cyber vulnerabilities.

PWP believes that any legislative efforts should focus on providing information to those in charge of the nation's critical infrastructures. NERC works closely with DHS and other agencies, but more sharing of information is needed. For example, the bulk power system was exposed to the "Aurora" vulnerability for three years before the electric industry received actionable information from federal government. Timely sharing of critical information enables the electric power industry to take immediate action directing expert operators and cybersecurity staff to adjust systems and networks to ensure the reliability and security of the bulk power system.

Pasadena opposes any bill that would subject the electric sector to compliance with two separate sets of standards, one to avoid fines and penalties from FERC; and a second for liability protection from a federal cause of action. The electric power industry is fully committed to maintain and improve the security and reliability of the bulk power system, and stands ready to work with Congress, FERC, NERC, and other government agencies on these critical issues.

Therefore, we urge you to support changes that would provide timely sharing of critical information and preserve the existing NERC-FERC models for developing mandatory cybersecurity standards. Our business depends on a reliable and secure bulk power system.

PWP provides the following general comments on the Framework, and answers to a number of the specific questions below.

## I. General Comments on the Framework

PWP believes that any legislative efforts should focus on providing information to those in charge of the nation's critical infrastructures. As an electric utility which owns and operates facilities that are part of the Bulk Electric System and subject to Section 215 of the Federal Power Act, 16 U.S.C. 824o, PWP is subject to reliability standards developed by the NERC and approved by the FERC. These NERC Critical Infrastructure Protection ("NERC CIP") standards were developed through an industry consensus-based standards development process that has been accredited by the American National Standards Board ("ANSI").

Unlike the cyber security standards described in the EO that may be developed pursuant to a final NIST Cybersecurity Framework, NERC CIP reliability standards impose mandatory and enforceable requirements on owners and operators of the Bulk Electric System, as set forth in the applicability sections of these standards. Compliance with NERC CIP standards is enforceable by NERC, subject to FERC oversight and approval. Enforcement actions may entail the imposition of financial penalties of up to one million dollars per violation per day, as well as NERC remedial action directives to ensure immediate changes to cyber security practices and procedures.

PWP sees significant value in the NIST RFI proposal to develop and publish a cross-sector supplemental baseline Cybersecurity Framework, but strongly urges NIST to recognize the breadth and depth of NERC's existing CIP standards, and to ensure that the NIST Framework steers clear of conflict or duplication, either of which could lead to confusion and compromise security. NERC works closely with DHS and other agencies, but more sharing of information is needed. The Framework should encompass and not conflict, with existing Critical Infrastructure Protection ("CIP") Standards promulgated by independent regulatory agencies. Pasadena opposes any bill that would subject the electric sector to compliance with two separate sets of standards. A specific statement indicating that the recommendations embodied in the Framework are not intended to conflict with existing law, regulatory authorities or regulations would provide a clear signal that no conflict is intended.

## II. PWP Responses to NIST RFI Questions

### A. NIST RFI Section 1: Current Risk Management Practices.

- Question 1: What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

The biggest impediments to our ability to take appropriate action to address threats and vulnerabilities are the lack of actionable and timely information from the federal government and the complexities associated with legal protections for the secure communication between government and industry of highly sensitive information about cyber-security vulnerabilities, without fear of public disclosure. The current priority is the need for timely, actionable

information regarding existing and emerging threats, and sound input regarding appropriate responses. For some years, it has been clear that the intelligence community and other governmental agencies have had access to a good deal of information that has not been widely shared with the private sector such as the "Aurora" example given previously. Of course, the electric utility sector has been on the front line in experiencing vulnerabilities and devising solutions, using the resources available to us based upon our respective self-assessments of the vulnerabilities we face and threats we receive. Yet there is no substitute for a clearinghouse for information and programs which will ensure that the nation can collectively learn from individual experiences. Accordingly, the electric industry places high on the list of challenges the need for information sharing between the federal government, intelligence community and the private sector, and the timely dissemination of information on emerging threats and responses to those threats.

As a model for this framework, PWP would like to point to NERC's Electricity Sector - Information Sharing and Analysis Center ("ES-ISAC"). We have found this program to be a valuable source of reliable information often not available elsewhere. The ES-ISAC has also substantially improved the efficacy of its communications infrastructure and made major strides to reach a greater number of large and small entities across the electricity subsector. However, much more can be done to improve the content of the information provided by the sub-sector's federal partners to the ES-ISAC and to begin more effective informational exchange across critical infrastructure sectors. The effectiveness of the process can be improved as more actionable intelligence is shared by federal agencies with the electricity sector, particularly when such information can be redacted on a timely basis to allow classification of such information as non-public, For Official Use Only ("FOUO"). Only then will private sector entities be able to leverage knowledge into effective risk-based cybersecurity practices.

- Question 2: What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

PWP has been active in advocating for legislation to address both issues and we welcome the EO's directive to the Secretary of Homeland Security and the Attorney General to establish a process providing for the rapid dissemination of unclassified and classified information relevant to cyber vulnerabilities, along with information available under the Cybersecurity Services program, to critical infrastructure entities. Establishing strong information sharing practices between federal government agencies charged with ensuring domestic security, the intelligence community and industry is essential in protecting critical assets from intrusion and disruption. To date much of this information has been shielded from entities seeking to manage cyber vulnerabilities.

As discussed in general comments above, a cross-sector framework must be sufficiently flexible to enable varied organizations to be agile in responding to ever-evolving threats, and a wide range of risks. The Framework must be flexible, goals-based and process- oriented, while avoiding overly prescriptive approaches or technologies that risk becoming antiquated, and are not scalable to a realistic evaluation of risk. Too rigid a Framework would risk establishing

perverse incentives to develop and stick with programs and practices that fail to respond appropriately to evolving risks.

- Question 3 – NA
- Question 4 - NA
- Question 5: How do organizations define and assess risk generally and cybersecurity risk specifically?

As a member of the electric utilities industry, risk is generally defined as a function of the likelihood that the reliable real-time delivery of electric power will be disrupted, particularly if such disruptions occur on a wide area basis for an extended period of time. Reflecting this basic concept, DOE's RMP guideline – developed in conjunction with NIST, NERC and the electric subsector – defines "Cybersecurity Risk" as

[t]he risk to organizational operations (including mission, functions, image, reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or [information technology] and [industrial control systems].[i]

- Question 6 – NA
- Question 7: What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

As part of the electricity subsector, PWP is obligated to comply with mandatory NERC CIP standards. In addition, useful work has been done by DOE in outlining essential capabilities and organizational tools through the ES-C2M2 Maturity Model, and the RMP, discussed below.

1. NERC CIP Standards

The electricity subsector is subject to NERC's mandatory CIP standards, including prescribing standards addressing both cybersecurity and physical security. The body of CIP standards was developed by NERC in a cooperative process with the electric industry, approved by FERC pursuant to Federal Power Act Section 215, and currently is mandatory and enforceable, carrying with it potential financial penalties of up to $1 million per day, per violation. The Electric Trade Associations urge NIST to be mindful of the comprehensive protections woven into the current regulatory regime, including the CIP standards, and to ensure that any Framework ultimately developed does not inadvertently undermine existing cybersecurity controls that apply to the electric subsector.

## 2. DOE ES-C2M2 and RMP

PWP commends to NIST's attention DOE's ES-C2M2 Model, along with the RMP, developed by DOE, in collaboration with NIST, NERC, the Department of Homeland Security and the electric industry. The Maturity Model was designed to support ongoing development and measurement of cybersecurity capabilities within the electric subsector by: (a) strengthening this subsector's cybersecurity capabilities; (b) enabling utilities to effectively and consistently evaluate and benchmark cybersecurity capabilities; (c) sharing information and best practices within the subsector as a means of improving cybersecurity capabilities; and (d) enabling electric utilities to prioritize actions and investments to improve cybersecurity. Also discussed above, the RMP provides an organizational framework for addressing risk, counseling the use of organizational and technical tools scaled to each responsible entity's evaluation of risk. Because these models do not endorse particular methodologies or technologies, they are sufficiently flexible to enable organization to respond to evolving threats, while scaling their programs to an evaluation of risk. The models do not reflect a checklist approach to particular tools or technologies, which would ultimately be counterproductive in inhibiting the agility needed to respond to an always changing environment.

- Question 8: What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

Section 215 of the Federal Power Act (FPA) provided for FERC's certification in 2006 of NERC as the nation's Electric Reliability Organization ("ERO"). FPA section 215 requires users, owners and operators of the bulk power system within the U.S. to comply with mandatory and enforceable reliability standards developed by NERC and approved by FERC, including the body of CIP standards which, as noted above, prescribe a core set of mandatory baseline protocols for protection of critical cyber and physical assets. As part of this reliability framework, NERC has legal authority to monitor and enforce compliance with FERC-approved reliability standards, and to assess penalties and sanctions. In addition, FERC maintains independent authority under the statute to monitor and enforce the reliability standards.

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

PWP agrees with NERC that, for its part, the electric subsector shares certain interdependencies with cyber assets in both the communications and transportation sectors. Among other things, critical assets in the electric subsector that are potentially interdependent on the communications and transportation sectors include industrial control systems, energy marketing and management systems, as well as generation, transmission and distribution systems.

- Question 10: What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

NERC's body of Emergency Operations Planning ("EOP") reliability standards (part of the CIP suite of standards) address operational resilience and restoration in the electric subsector through requirements for, among other things, the backup and recovery of energy systems.

- Question 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?

PWP is compliant with NERC CIP standards, which have embedded within them various reporting requirements with regard to disturbances or unusual occurrences, suspected or determined to be caused by sabotage (*i.e.*, CIP-001-2).

Specifically, CIP-001-2 calls on PWP to report to relevant government and regulatory bodies disturbances or unusual occurrences that are suspected or determined to be caused by sabotage. The standard, too, requires PWP to establish communications contacts with local Federal Bureau of Investigation officials, and to develop reporting procedures.

- Question 12: What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

NERC currently plays a key role in overseeing and enforcing industry compliance with CIP standards through well-established processes and procedures rooted in Federal Power Act Section 215. In addition, NERC and the electric subsector actively develop and refine mandatory cybersecurity standards aimed at threat identification and protection of key physical and cyber assets. As NERC points out in its comments, the CIP standards create a baseline for stakeholders to adopt security best practices and resources into their organizations, while remaining sufficiently flexible to account for the dynamic nature of technology and emerging threats. NERC and the ES-ISAC facilitate this process by providing tools to industry which are essential to the electric subsector's ability to effectively assess new threats and vulnerabilities.

PWP endorse NERC's work in this area and urges NIST, in developing the Framework, to draw on NERC's substantial technical expertise and knowledge of critical infrastructure cybersecurity assessment, monitoring, standards development, and oversight.

## B. NIST RFI Section 2: Use of Frameworks, Standards, Guidelines and Best Practices.

- Question 1: What additional approaches already exist?

As NIST moves forward to develop a uniform cyber Framework, PWP sees much value in 5 existing approaches in the electric subsector: (1) the NERC CIP standards; (2) DOE's ES-C2M2; and the (3)DOE RMP guideline, (4) NERC and Regional Critical Infrastructure Protection Committees (CIPC), and the (5) ES-ISAC alert process.

Discussed above, the CIP standards focus on cybersecurity and physical security of cyber assets. The DOE ES-C2M2 model, developed in collaboration with NIST, NERC, the Department of Homeland Security and the electric industry, is designed to support ongoing development and measurement of cybersecurity capabilities within the electric subsector, while the companion DOE RMP guideline is intended to provide a viable risk management process that is tailored to the needs of electric subsector organizations. The Electric Trade Associations' members fully endorse these three approaches.

The existing NERC and Regional CIPC working groups provide valuable industry input to the development of guidelines and best practices. These groups will provide the needed resources in the form of subject matter expertise. The ES-ISAC provides the real time threat landscape and triage of specific Electricity Sub-sector mitigation methods through a "Hydra" group. The Hydra group evaluates real time threats and gives input on the Alerts that are sent out by the ES-ISAC.

- Question 2: NA

- Question 3: Which organizations use these approaches?

The NERC CIP standards, and indeed the entire body of NERC reliability standards, apply to all "users, owners and operators" of the Bulk Electric System ("BES"), pursuant to Section 215(b) of the Federal Power Act. The BES is given specific definition in the NERC standards, and generally encompasses facilities operating or interconnected at voltages of greater than 100 kV. Federal Power Act Section 215(a) provides that the NERC reliability standards do not apply to "facilities used in the local distribution of electric energy."

Both the DOE ES-C2M2 and companion RMP guidelines are electric-subsector-wide documents that list core capabilities, and outline organizational tools for assessing and managing cyber risks.

The NERC registered entities comprise the NERC and Regional CIPC's focus on BES cyber and physical security issues.

- Question 4: What, if any, are the limitations of using such approaches?

The NERC CIP standards, pursuant to Federal Power Act Section 215, are designed to ensure the reliable operation of the bulk power system. Reliability standards apply to all "users, owners and operators of the bulk-power system"; by statute, they do not apply to "facilities used in the local distribution of electric energy". Nor do they apply to the various business-related cyber systems used by our members that are not used in the real-time operation of the bulk electric system.

However, many of the Electric Trade Associations have helped educate smaller entities such as PWP on the benefits of wider application of NERC CIP standards to our non-BES operations. For example, many of the NERC standards in CIP Version 5 could be applied on a voluntary basis to distribution system operations. More generally, the NERC CIP standards provide for the establishment of organizational cybersecurity policies and programs that are appropriate for many organizations that operate cyber systems in an industrial control system environment.

*The DOE ES-C2M2 and RMP guidelines apply to the entire electricity subsector, which includes entities involved in the generation, transmission, distribution, and marketing of electricity.*

- Question 5: What, if any, modifications could make these approaches more useful?

As noted, the owners, operators and users of the Bulk Electric System participate in NERC's ES-ISAC alert system. This program may be substantially enhanced when, as directed by the EO, federal agencies coordinate the release of timely information possessed by the government regarding existing and emerging threats. Also worthy of consideration would be participation of non-NERC registered entities in the ES-ISAC and creation of regional/state cyber/physical security working groups outside of the NERC process, which are developed on frameworks similar to those by NERC and the NERC Regions.

- Question 6: How do these approaches take into account sector-specific needs?

Both the NERC CIP standards and the DOE ES-C2M2 Model were developed with the specific needs and requirements of the electric subsector in mind. The NERC standards are developed using an ANSI-accredited standards development process, the core of which is a consensus-based approach to standards development which draws on the technical expertise and experience of the electric industry stakeholders. The CIPC's and the ES-ISAC are limited to the electricity sector only.

- Question 7: When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

PWP would like to note that the NERC reliability standards are mandatory. There is a role for supplemental voluntary practices, needed in order to respond flexibly to emerging threats. As a member of The Electric Trade Associations, PWP cautions against the creation of a second set of potentially conflicting standards.

- Question 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 coordination of the regional fusion centers for information exchange.

- Question 9: What other outreach efforts would be helpful?

As noted by NERC in its RFI comments, additional outreach efforts by the sector-specific-agencies, Government Coordinating Council and Sector Coordinating Council is essential. Specifically, these groups should be involved in developing and sponsoring a collaborative, comprehensive outreach effort, which informs sector stakeholders on key structures, policies, priorities and approaches employed within that sector. Sector-specific-agencies, too, should ensure that proper resources are devoted to sector priorities, and be sure to disseminate and publish as much outreach content as possible.

### C. NIST RFI Section 3: Specific Industry Practices.

PWP would like to note that the nine industry practices identified by NIST[1] are widely used throughout the electric subsector, and are reflected within the body of NERC's currently-effective CIP standards, CIP-002 through CIP-009. In this regard, PWP endorses NERC's position that these CIP standards outline specific actions to be undertaken by asset owners and operators to protect critical cyber assets necessary for electric system reliability.

PWP agrees with NERC that a key implementation challenge faced by the electric sub-sector is ensuring that entities adequately secure their operational systems (*e.g.*, control systems, SCADA, etc.) from potential threats and vulnerabilities introduced by an increased reliance on interoperable operating systems and networks without compromising the efficiencies and reliability benefits offered by those systems.

## III. Conclusion

PWP is in full support of the work NIST has undertaken to develop a Cybersecurity Framework consistent with the EO, and asks that these comments be reflected in the shape of the Framework.

Respectfully submitted,

for Angela Kimmey
NERC Compliance Officer
City of Pasadena Water and Power

[1] The nine specific industry practices identified by NIST in the RFI are these: (1) separation of business from operational systems; (2) use of encryption and key management; (3) identification and authorization of users accessing systems; (4) asset identification and management; (5) monitoring and incident detection tools and capabilities; (6) incident handling policies and procedures; (7) mission/system resiliency practices; (8) security engineering practices; and (9) privacy and civil liberties protection.