TACOMA PUBLIC UTILITIES
3628 South 35th Street
Tacoma, Washington 98409-3192

April 10, 2013

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

Dear Ms. Honeycutt:

Please accept these comments submitted by Tacoma Public Utilities (TPU) in response to NIST docket number 130208119-3119-01, "Developing a Framework to Improve Critical Infrastructure Cybersecurity." We regret our late response but hope you will find our feedback helpful as NIST develops a framework to reduce cyber-risks to critical infrastructure. As a member of the American Public Power Association (APPA) and the Large Public Power Council (LPPC), Tacoma Public Utilities supports the comments submitted by those entities.

As background, TPU is the municipally owned utility of the City of Tacoma. TPU provides electricity, drinking water, rail and telecommunications to tens of thousands of customers within the City of Tacoma and throughout incorporated and non-incorporated communities throughout Pierce and King Counties in Washington State.

As you know, Tacoma Public Utilities is required to comply with mandatory and enforceable federal electric reliability standards that are specifically designed to protect the electric grid from reliability risks, including physical and cyber-attacks. The North American Electric Reliability Corporation (NERC), designated by the Federal Energy Regulatory Commission (FERC) as the electric reliability organization under the Federal Power Act (FPA), enlisted teams of industry subject-matter experts and responded to FERC directives to create mandatory and enforceable Critical Infrastructure Protection standards ("CIP Standards") for the bulk electric system (BES).

The electric power industry as a whole and Tacoma Public Utilities in particular has a long history of reliably serving our customers. The accountability we have to our citizen-customers provides us with constant motivation to maintain a reliable, low-cost system. Because each utility has unique operational designs and needs, we believe that industry expertise and public-private information sharing is critical to cybersecurity protection planning and implementation. We remain interested in working with the federal government and our regulators to create and actively participate in a robust system of information sharing between federal intelligence communities and our industry. Enhanced information sharing is a key component to strengthening the protection of the bulk electric system moving forward.

TACOMA POWER
TACOMA WATER
TACOMA RAIL

Should you have any questions, please contact myself, Clark Mather, at 253-441-4159. We look forward to working with you as the process laid out in Executive Order 13636 moves ahead.

Sincerely,

Clark Mather
Senior Manager for External Affairs

Tacoma Public Utilities
NIST Cybersecurity Framework RFI Comments

Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

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

TPU and our industry generally continues to place 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 actionable information on emerging threats and vulnerabilities as well as responses. This information includes the granting of additional, and in some cases higher-level, security clearances for electric utility representatives.

Additionally, mapping of critical infrastructure points of reliance, and building communication channels around those is also recommended. Appropriate controls on information disclosure must also be implemented.

An example of an effective collaborative information exchange is the Public Regional Information Security Event Management (PRISEM) system. This system is an online early-warning system that aggregates and analyzes real-time cyber event information across the Puget Sound metropolitan area - for federal, state and local government; universities; and private sector partners. Member organizations include, Snohomish Public Utilities District, Seattle City Light, Children's Hospital, Port of Seattle, Port of Tacoma, and more.

Vendor management and oversight is another factor in cybersecurity risk management. Cybersecurity must become an integral part of the development, manufacturing, distribution and support systems of our vendors. Vendor requirements should address secure product development, secure manufacturing, distribution, and continued support for security patching throughout the product lifecycle. Incentives for vendors in the Industrial Control Systems space to support a new framework could go a long way in making this happen.

Another concern is the historical industry focus on availability. This was done, at least in part, by removing device complexity to reduce the risk of device failure. This has the potential of leaving devices insecure due to lack of necessary support for basic security controls such as complex passwords, access logging, and link encryption. The focus on availability can leave historical devices exposed. Because of the critical nature of the electricity subsector's service delivery, replacement of these assets must be done systematically and over a period of years.

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

While a one-size-fits-all approach may be desired, the reality is that each sector and organization has its own specific set of risks, and therefore must provide its own set of controls. Under a cross-sector approach, incorporating appropriate controls for these disparate risks in a meaningful way may be the greatest challenge. Another challenge will be regional and cross-sector information sharing.

General information security frameworks exist, such as, ISO27000, ITIL, COBIT v5, Common Criteria and SANS 20 Critical Security Controls.

The implementation of any of these standards is up to the organization, and as such varies greatly between like organizations. However, there are obvious similarities in taxonomy between organizations that deliver based on the same standard (i.e. ISO27001) which benefits those organizations by speaking the same security "language."

Unfortunately, these frameworks or standards do not address the necessary regional and cross-sector information sharing required to better address critical infrastructure cybersecurity needs.

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?

Tacoma Power's Internal Compliance Program (ICP) is the governing document applicable to all employees who perform functions that directly or indirectly affect any portion of the BES. The ICP describes the steps undertaken by Tacoma Power to implement its commitment to the reliable operation of the BES in compliance with all federal laws and regulations and applicable North American Electric Reliability Corporation (NERC) Reliability Standards as approved by FERC. This document describes how Tacoma Power institutionalizes the compliance program and contains references to the documented plans, policies, procedures, and other systematic

preventive measures used for governance, management, and operations. The program is managed by the Reliability & Compliance Manager with oversight and guidance provided by the Reliability & Compliance Governance Committee (RCGC). The RCGC includes the Tacoma Power Superintendent, the RCM, R&C Senior Supervisor, TPU legal counsel, and the manager of each of Tacoma Power's business units. The Tacoma Power Superintendent chairs the RCGC.

4. Where do organizations locate their cybersecurity risk management program/office?

Tacoma Power's cybersecurity risk management program resides in a business unit, managed by the CIP Senior Manager, which contains system administrators and reliability & compliance (R&C) personnel. R&C assesses CIP compliance and risk, based on likelihood and consequences, while system administrators implement and perform processes to ensure compliance with NERC Reliability Standards for the system.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

For electric utilities, risk is generally defined as a function of the likelihood that the delivery of electric power will be disrupted. 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]."[1]

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Cybersecurity is fully incorporated into the organization throughout Tacoma Power. Each system or facility is assessed prior to new equipment being introduced into the current infrastructure. Hardware, software, and other changes to the system are tested and/or assessed for all changes to Tacoma Power's CIP system. Routine vulnerability

[1] DOE RMP guideline at 66.

assessments are conducted at least annually to incorporate all devices in the CIP system.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

Tacoma Power adheres to the NERC-CIP Standards:

CIP-001-2 – Sabotage Reporting
CIP-002-3 – Critical Cyber Asset Identification
CIP-003-3 – Security Management Controls
CIP-004-3 – Personnel & Training
CIP-005-3 – Electronic Security Perimeters
CIP-006-3 – Physical Security of Critical Cyber Assets
CIP-007-3 – Systems Security Management
CIP-008-3 – Incident Reporting and Response Planning
CIP-009-3 – Recovery Plans for Critical Cyber Assets

Additional resources utilized are:

- DOE Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline
- DOE ES-C2M2 (Electricity Subsector – Cybersecurity Capability Maturity Model)
- NERC ES-ISAC (Electricity Sector Information Sharing and Analysis Center
- ICS-CERT
- ISO 27002
- SANS 20 Critical Controls

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?

Tacoma Power as a Bulk Power System owner/operator is regulated by the North American Electric Reliability Corporation (NERC) Reliability Standards, per Section 215 of the Federal Power Act. The NERC CIP Standards reflect the cybersecurity standards enforced by NERC. NERC has delegated the enforcement authority to eight regional entities. The Western Electricity Coordinating Council (WECC) has responsibility for Tacoma Power. Tacoma Power is responsible for reporting to WECC, NERC and FERC.

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

Tacoma Power is dependent upon the water and transportation sector services, and has some reliance on the communications sector. However, like many utilities, much of Tacoma Power's communications infrastructure is on a private network. Many of the local critical infrastructure sectors within the region are dependent upon Tacoma Power's service delivery.

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

Tacoma Power has developed a strategic plan that maps out the organization's goals and initiatives short and long term. Emphasis have been placed on areas that support managing cybersecurity risk, such as; manage IT assets, leverage and enhance technology, and maintain a focus on compliance and safety. These goals cascade down to the business unit goals and ultimately to the individual employee goals, each level of performance supporting the overall goal. Quarterly assessments by senior management help identify areas where greater controls or attention may be needed.

Key Performance Indicators (KPI) are a method to measure the performance of a system. Because Tacoma Power falls under NERC Reliability Standards enforcement, each of the requirements provides a KPI to measure performance. Enforcement is based on a 100% compliance level, with penalties for non-compliance.

Tacoma Power has developed KPIs associated with the CIP cybersecurity standards and requirements.

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?

Tacoma Power as a Bulk Power System owner/operator is regulated by the North American Electric Reliability Corporation (NERC) Reliability Standards, which are enforced by WECC within the region. These standards have embedded within them various reporting requirements with regard to disturbances or unusual occurrences, suspected or determined to be caused by sabotage, as well as cybersecurity incidents related to critical cyber assets. Tacoma Power is also required to report cybersecurity incidents to the NERC ES-ISAC. The ES-ISAC also routinely exchanges information with leading industry technology and services vendors. Any regulatory related information gets reported to WECC who reports it to NERC who then reports it FERC.

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

Assessment of standards conformity is seen as a necessity. Within the Electricity Subsector, NERC has delegated assessment to the eight regional entities.

There are certification programs for many of the general frameworks mentioned in question #2, (i.e. ISO certification,) however the maturity of these certification programs is not on par with the standards they are meant to certify. There is no inherent consistency between the programs of certified businesses. The reason for this may be that the entities being assessed are responsible for specifying the scope of their protected environment themselves. If this concept were replaced with a sector-specific risk based scope, as seen with the NERC-CIP Standards, the assessments could be effective.

Additionally, these assessment bodies are maturing, and expanding as businesses addresses their need to prove their security readiness. They are therefore not currently staffed sufficiently to provide this assessment authority to a larger scope.

In the electricity subsector, 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 electricity 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.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

General Information Security Frameworks:

- ISO 27000 Information Security Management
- ITIL
- Common Criteria
- Cobit v5
- SANS 20 Critical Security Controls

Federal Guidelines:

- NIST FIPS 200 & SP 800-53

Industrial Controls based:

- ISA-99 Security Guidelines
- NIST SP 800-82

Electricity Subsector Specific:

- NERC CIP Standards
- ES-C2M2 (DOE - Electricity Subsector Cybersecurity Capability Maturity Model)
- DOE Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline

2. Which of these approaches apply across sectors?

All of the above have applicability cross-sector. The electricity subsector specific examples can easily be tailored to more general frameworks.

3. Which organizations use these approaches?

The general approaches are in use globally by thousands of organizations in many business sectors.

NERC Reliability Standards apply to all "users, owners and operators" of the bulk power system (BPS), which is the subset of the Electricity Subsector that deals with reliability of the transmission network, generally including the parts of the electric grid responsible for higher voltage and larger quantities of electricity activity. As provided in Federal

Power Act Section 215, the NERC Standards do not cover "facilities used in the local distribution of electric energy."

4. What, if any, are the limitations of using such approaches?

The more general standards or frameworks are limited by the application of the standard to individual organizations, and the authority of the governing bodies providing certification or accreditation. Without regulation, these frameworks can be misused or misapplied, and do not provide the consistency of delivery sought through this process. Vendor management is typically not addressed by these frameworks or approaches. In the case of critical infrastructure, lack of proper vendor management and oversight is a key facet of the cybersecurity risk. In addition, timely access to actionable threat and vulnerability information will go far to ensure organizations are more agile both in their ability to respond to emerging threats, and to adjust their control selections ahead of formal guidance.

5. What, if any, modifications could make these approaches more useful?

Providing regulatory authority for setting the mandatory standards for the resulting framework will go a long way in providing the desired consistency of cybersecurity, much like what has been achieved in the Electricity Subsector through NERC-CIP.

Additional processes must also be developed for information sharing at the national, regional and local levels.

Adding vendor management is also seen as a useful modification.

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

The NERC CIP's identified the critical assets and associated cyber assets that relate to the reliable operation of the bulk electric system (BES). This methodology took into account the unique attributes of the electricity subsector and the BES and developed controls that do not inhibit the availability requirements of the systems. The DOE RMP and ES-C2M2 guidelines that were developed specifically for the electricity sector include the determination of the different disciplines within the sector (e.g. energy generation, transmission, distribution, buying and selling markets and corporate operations).

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

We note that current NERC reliability standards are mandatory. Sector-specific standards should be applied to existing frameworks, since each sector has a different threat and vulnerability profile. While many real-time systems, as employed in the electricity subsector, have analogues in other sectors, there are many systems that are dissimilar.

Where there is an existing mandatory framework in place, like the electricity subsector's NERC-CIP, care must be taken in not forcing adherence to dual standards, or creating standards that might conflict with current requirements.

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 sector-specific agencies (SSA) and coordinating councils (CC) can play an important role in communicating with industry on the threats and vulnerabilities. Since the SSA's and CC's have a closer alignment with the operations of their sector, they have a unique opportunity to bring together industry to develop case studies related to the implementation and adoption of the framework. These case studies can be used to develop uniformity across the sector. The SSA's and CC's have specific understandings of the unique attributes of their sector and can assist with the development of risk based measures so the adoption of the framework is commensurate with risk and operations of the sector organization.

9. What other outreach efforts would be helpful?

The SSA's and CC's can be the coordinators in the establishment of the public-private partnerships with industry as well as establishing collaboration across sectors. Where there are interdependencies between critical infrastructures, there is an opportunity for the SSA's and CC's to create information sharing and analysis that can be used to facilitate cross-sector understanding of threats and vulnerabilities. The SSA's and CC's can leverage economies of scale across sectors to improve the overall national cybersecurity posture. Using the Information Sharing and Analysis Centers (ISAC) for each sector, organizations can share with the ISAC specific log information that the ISAC can then use to correlate events across their sector and create reports and analysis as needed. Additionally, the SSA's and CC's can be an aggregator among the different critical infrastructures of log information to create a view across sectors and across interdependent sectors. From a public-private perspective, developing this scale

of bi-directional security information has the potential to dramatically increase the security posture of each sector and the nation.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

1. Are these practices widely used throughout critical infrastructure and industry?

The nine practices listed in the RFI are in use by Tacoma Power and widely used throughout the Electricity Sub-sector and addressed within the current NERC-CIP Standards. NERC Standards, CIP-002 through CIP-009, provide specific actions for owners and operators to perform to protect critical cyber assets that support reliable operation of the bulk power system (BPS). These standards recognize the differing roles of each entity in the operation of the BPS, the criticality and vulnerability of the assets needed to manage BPS reliability, and the risks to which they are exposed. Many of the concepts within the CIP Standards are generic in nature and agnostic towards specific technology regarding security solutions.

2. How do these practices relate to existing international standards and practices?

The new NERC-CIP Standards (Version 5) generally cover the same subject areas as both the NIST FISMA framework and the ISA-99 Standards, along with the standards that they also reference.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

All of these practices are important for the secure operations of critical infrastructure. It is the degree of implementation that needs to be managed to ensure that implementation of these controls do not impede the reliable operations of the systems and business processes. The degree of implementation needs to be balanced with the overall risk (i.e. threats, vulnerabilities, and likelihood/consequence of harm) to the systems.

Referencing the specific practices listed in this section, the "separation of business from operational systems" is one of the most critical controls for the secure operation of critical infrastructure. The implementation of this practice can greatly reduce the overall attack surface. It is important for organizations to use this practice to create a clear demarcation in their network and system architectures. The sensitivity related to operational systems is much different than the sensitivity related to corporate systems.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

All of these controls are applicable cross-sector.

5. Which of these practices pose the most significant implementation challenge?

The most significant implementation challenge within the bulk power system is ensuring that entities adequately protect their operational systems (control systems, SCADA, etc.) from un-trusted sources.

The most significant implementation challenge, within the listed practices above, involve the "monitoring and incident detection tools and capabilities" practice. Recent events in multiple sectors have demonstrated that advanced persistent threats (APT) have significant, technically-capable personnel and sufficient resources to attack and overcome some of the most dedicated security programs in the world. However, defenders against APT attacks are often at the other end of the scale in terms of personnel and resources, both in-house and through third parties. Threat information sharing between government and industry is extremely important, but—even with robust tools and capabilities to monitor and detect incidents within critical infrastructure controls and systems—the security threat from APTs is continually evolving with new methods of attack.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

All Electricity Sub-sector participants that are users, owners and operators of the bulk power system are required to follow all NERC Reliability Standards, including the Critical Infrastructure Protection standards. Entities also voluntarily follow guidance developed and issued by NERC and others such as NIST, International Society of Automation (ISA), International Electrotechnical Commission (IEC), and the International Organization for Standards (ISO).

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Tacoma Power has developed a mature program to manage IT standards to maintain compliance to NERC Standards and Requirements. Tacoma Power has a Reliability and Compliance organization, as well as project management office to manage both the compliance implications and delivery of IT projects. Both utilize standard methodologies in delivering on their responsibilities to the organization. Delivering on the NERC-CIP requirements provides an information security management system to the business.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Tacoma Power has developed a Cybersecurity Incident Response Plan to address the escalation needs in the face of a cybersecurity incident.

Additionally, Tacoma Power complies with NERC CIP standards, which requires reporting for significant incidents to the ES-ISAC.

The NERC Alert System addressing such matters has been implemented and formalized across the industry for registered entities. As defined by NERC Rules of Procedure, alerts are divided into three distinct levels:

1. Industry Advisory - Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary

2. Recommendation to Industry - Recommend specific action be taken by registered entities. Require a response from recipients as defined in the alert

3. Essential Action - Identify actions deemed to be "essential" to bulk power system reliability. Requires NERC Board of Trustees approval prior to issuance. Similar to recommendations, essential actions also require recipients to respond as defined in the alert

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

City of Tacoma, dba Tacoma Public Utilities is a municipal organization that is subject to Washington State public disclosure requests. Washington State code RCW 42.17.310, exempts municipal organizations like Tacoma Power from disclosing information regarding critical infrastructure.

Risks may include sharing sensitive information regarding authorization of users accessing systems. Individuals' names are tied to the authorizations, which may raise privacy and civil liberties concerns, particularly if an incident occurs.

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

Not Applicable.

11. How should any risks to privacy and civil liberties be managed?

Information sharing should be managed, removing any PII (or BII) information, from publicly disclosed notifications. ISAC organizations should be cognizant of any regulatory implications, and work to maintain privacy.

Regulatory and Federal organizations should support open sharing without risk to privacy or compliance implication.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

From the SANS 20 Critical Security Controls by order of delivery preference:

- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Malware Defenses
- Application Software Security
- Wireless Device Control
- Data Recovery Capability
- Security Skills Assessment and Appropriate Training to Fill Gaps
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Limitation and Control of Network Ports, Protocols, and Services
- Controlled Use of Administrative Privileges
- Boundary Defense
- Maintenance, Monitoring, and Analysis of Audit Logs
- Controlled Access Based on the Need to Know

- Data Loss Prevention
- Penetration Tests and Red Team Exercises

Additionally as stated earlier, vendor management and information sharing are key areas of concern.