Department of Water and Power the City of Los Angeles

ANTONIO R. VILLARAIGOSA
Mayor

Commission
THOMAS S. SAYLES, *President*
ERIC HOLOMAN, *Vice President*
RICHARD F. MOSS
CHRISTINA E. NOONAN
JONATHAN PARFREY
BARBARA E. MOSCHOS, *Secretary*

RONALD O. NICHOLS
General Manager

April 8, 2013

Ms. Diane Honeycutt
National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive, Stop 8930
Gaithersburg, Maryland 20899

Dear Ms. Honeycutt:

Subject: Developing a Framework to Improve Cybersecurity for Critical Infrastructure

The Los Angeles Department of Water and Power (LADWP) appreciates the opportunity to respond to the Request for Information (RFI) issued by the National Institute of Standards and Technology and published by the Federal Register on February 26, 2013.

LADWP is the largest municipal water and power utility in the nation, and was established more than 100 years ago. LADWP delivers reliable, safe water and electricity to approximately 3.8 million residents and businesses in the City of Los Angeles.

LADWP welcomes the initiative expressed in Executive Order 13636[1] (Executive Order), to provide the private sector entities with actionable information on emerging threats. LADWP also welcomes the opportunity to assist in the creation of a voluntary program to support the adoption of the Cybersecurity Framework (as envisioned in the Executive Order) by owners and operators of critical infrastructure.

From an electricity sector perspective, the development of a Cybersecurity Framework should be careful not to conflict with existing mandatory and consensus-based Critical Infrastructure Protection (CIP) Standards developed by the North American Reliability Corporation (NERC) and approved by the Federal Energy Regulatory Commission pursuant to Section 215 of the Federal Power Act. These CIP Standards prescribe a core set of mandatory baseline requirements for critical energy infrastructure.

[1] "Executive Order 13636 – Improving Critical Infrastructure Cybersecurity" 78 FR 11739 (February 19, 2013)

The Cybersecurity Framework should establish a baseline set of goals and processes, and should not attempt to prescribe or even suggest specific methodologies or technologies. This seems to be contemplated by the Executive Order. This approach is important since:

- Cyber threats are constantly evolving and specific approaches or technologies will quickly become antiquated and counterproductive; and
- The Framework is designed to apply to various sectors, within itself facing a myriad of challenges.

LADWP has developed and implemented a robust cyber security program pursuant to the CIP Standards. LADWP ensures that it continuously remains in compliance with all aspects of the CIP Standards, and believes that these standards establish an important baseline for properly securing Bulk Power System assets. As additional measures to respond to potential cyber threats and vulnerabilities, LADWP fully supports NERC's alerts issued by the Energy Sector – Information Sharing and Analysis Center.

For the electricity sector, the Department of Energy's, Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2) offers a good starting point for the Framework, along with the DOE's companion Risk Management Process guideline.

Attached please find LADWP's responses to the three groups of questions in the order in which they appear in the RFI. LADWP appreciates the sustained efforts to improve the Nation's cybersecurity across all sectors as a matter of the national and economic security of the United States, and looks forward to contributing to this important effort.

Sincerely,

Randy S. Howard
Chief Compliance Officer - Power System
111 North Hope Street, Suite 921
Los Angeles, CA, 90012
Telephone Number: (213) 367-0381
Email: Randy.Howard@ladwp.com

MG:nsh
Enclosure
SUBMITTED VIA EMAIL TO: cyberframework@nist.gov

CURRENT RISK MANAGEMENT PRACTICES

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

Some of the greatest challenges in improving cybersecurity include:

- Improving cybersecurity threat information sharing between the Federal government and the public and private sectors.
- Establishing a highly effective workforce through development and training with knowledge and experience that combines cybersecurity, control systems, supervisory control and data acquisition (SCADA) systems and information technology (IT) skill sets, to effectively face adversaries that are highly skilled and increasingly capable.
- Establishing a unified and fully integrated corporate approach to proactively manage cybersecurity challenges across various sectors applicable to the organization (e.g. water and electricity sectors).
- Improving the engagement of manufacturers of hardware and software systems, so that their cybersecurity controls become a core requirement for their business practices.
- Addressing the large amount of legacy systems prevalent in the electric and water industries (e.g. SCADA systems), and whose complete replacement will require extensive planning and capital investment, which typically is achieved over several years.

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

A cross-sector critical infrastructure framework that is too flexible may fail to provide standards that effectively protect all critical infrastructure adequately. On the other hand, a cross-sector framework that is too rigid may require some sectors to implement standards that may not be applicable, or worse, detrimental to their mission.

Meeting the needs of all critical infrastructure sectors with a single, balanced, real-world framework could become a costly, resource-intensive endeavor; there is no existing “silver bullet” on this matter. It is a challenge in which future technology will continue to play an important role in resolving.

It should also be noted that life-cycles for control systems (such as water) are 15-30 years, and thus running under legacy control systems. These legacy systems have proven to be highly reliable, and requirements to comply with a cross-sector standard must be balanced with the challenge of replacing billions of dollars in aging infrastructure, not to mention the increasing regulatory compliance cost.

Finally, incentives may be a useful approach to motivate organizations to implement initial voluntary standards across sectors.

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?

LADWP has implemented various cybersecurity practices and policies, such as security awareness program, information and systems security, electronic mail management, and computer incident response.

LADWP policies are developed centrally. Individual standards are also developed centrally, in support of the general policies. Also, policies specific to each computing environment are also developed consistent with regulatory compliance requirements and operational needs.

Procedures are developed by the different business units, in support of business operations and in compliance to regulatory and policy requirements.

Furthermore, LADWP operates its Bulk Power System in accordance with NERC Reliability Standards, and include standards related to Critical Infrastructure Protection (CIP). Furthermore, LADWP has established a Cybersecurity Project Office (CPO), which, in turns, reports to LADWP's Power System Executive Management. The responsibilities of the CPO include:

- Assuring compliance with mandatory and enforceable CIP Standards and addressing ES-ISAC alerts related to cybersecurity concerns;
- Developing cybersecurity standards, policies & procedures;
- Auditing cybersecurity on critical systems with a potential for cyber exploitation; and
- Reviewing cybersecurity risks and recommending remediation.

In addition, LADWP's Water System overall risk assessment includes cybersecurity and physical security reviews applicable to the Water System facilities. Senior Management is actively engaged in assessing the overall security risk at Water System facilities, and sets the priorities for risk mitigations.

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

LADWP has had a strong cybersecurity program for over a decade, and as indicated above, has established a Cybersecurity Project Office, responsible for compliance with mandatory NERC CIP reliability standards. The headquarters of these offices are located in downtown Los Angeles.

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

LADWP attempts to value risk to the infrastructure by utilizing traditional methods to regularly identify vulnerabilities (utilizing conventional vulnerability assessment techniques), threats (attempting to keep current on active threat vectors), and opportunities (using both intrusion detection and results from the vulnerability assessment),

Cybersecurity risk is identified as those acts that may disrupt the reliable operation of the utility and create negative impact to the confidentiality, integrity, or availability of LADWP information or systems. LADWP further assesses these risks by determining the impact a system may have if it is compromised via disclosure, modification, or unavailability. Some of the measures LADWP uses include loss of competitive advantage, operational disruption, denial of service, financial loss, or legal transgression resulting from a disclosure, modification or system failure.

Ultimately, LADWP management makes the determination on what risks responses should be undertaken (i.e. mitigation, avoidance, or other acceptable responses).

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

Cybersecurity risk is fully incorporated into LADWP's enterprise risk management process. Every system must undergo a risk assessment before it is implemented, and thereafter at each upgrade cycle.

Also, access management to LADWP systems, information, and data is conducted by the operating groups, as established by cybersecurity risk policies.

For NERC CIP standards, LADWP mandates that each employee with access to critical cyber assets receive cyber security training on an annual basis.

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

LADWP uses the following standards, guidelines, practices and tools to understand and manage risk at the different LADWP organizational levels:

NERC CIP Standards - These standards focus on cyber and physical security of cyber assets, and include the following:

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

LADWP has also established internal cybersecurity guidelines and standards to complement or enhance NERC's mandatory standards, which include the following areas:

- Information Classification and Protection
- System and Network Administration
- Security Access Controls
- Virus Protection
- Software and License Management
- Computer Incident Response
- Password Administration
- Computer and Internet Usage
- Exceptions Procedure

LADWP also employs many Best Practices with regard to cyber infrastructure including:

- Defense in Depth Protection
- Layered Security on Perimeters using a multiple DMZ modes
- Firewalls and Application Firewalls
- IDS and IPS
- Malware and Antivirus protection
- Server Installation and Hardening Best Practice
- Desktop Installation Best Practice
- Host Vendor screening for compliance
- Host Vendor audits for compliance
- Internet Categorization Filtering
- Disaster Recovery and High Availability Strategy
- Backup / Retention Strategy

LADWP also uses a number of industry standard tools to analyze, review and manage cyber risks, including: TripWire, Symante Suite, CiscoWorks Software, HP OpenView, KIWI CatTools, Remedy, and others.

Finally, LADWP also uses the ISA 99 as a guiding document to provide best management practices in the operation and maintenance of the control systems within the Water System

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?

The NERC CIP Reliability Standards were established by Section 215 of the Federal Power Act, and made compliance with these standards mandatory and enforceable on users of the Bulk Power System.

NERC, as the Electric Reliability Organization designated by FERC pursuant to Section 215(c) of the Federal Power Act, has the legal authority in that role to monitor and enforce compliance with NERC Reliability Standards and to impose, subject to FERC oversight, penalties or sanctions for non-compliance. NERC has delegated certain activities to eight Regional Entities, which in LADWP's case is the WECC Regional Entity.

Further, the Incident Response requirements included in CIP-008-3 require utilities to report to the Electricity Subsector – Information Sharing and Analysis Center of suspected cybersecurity events.

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

LADWP's energy market and management systems, and various energy generation, transmission, and distribution systems could be affected by other critical sectors, such as telecommunications and transportation.

At LADWP, the Water System depends on the Power System energy. However, the Water System's facilities are designed with independent power backup systems to prevent prolonged inoperability, and thus allow continued flow of safe water.

In general, interdependency impacts from other sectors could affect the electricity sector (and the larger energy sector), including each of the sectors listed in the question, either with direct impacts, or by providing early advanced indications and warning of potential risks to the sector. These indications could be actionable, with timely mitigation guidance that could help reduce or eliminate threat exposure.

LADWP works closely with the WECC and NERC to insure the continued health and reliability of the interconnected grid.

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

In order to enhance its situational awareness, LADWP monitors information provided through the ES-ISAC. Furthermore, as part of LADWP's continuity of operations planning, it has identified those critical functions necessary to deliver electric power, and maintains plans for the restoration of those systems.

NERC has also developed operational standards for the energy-sector, including the Emergency Operations Planning (EOP) standards that address operational resilience through mandated backup and recovery goals. The EOP standards complement the CIP standards and are integrated into LADWP's objectives and operations.

LADWP has established cybersecurity processes and procedures to effectively support all IT security objectives (e.g., testing & deploying security patches and virus protection) so that no major IT security incidents occur at any facilities. Annual vulnerability assessments are performed to see an ongoing reduction of high- and medium-impact findings.

Furthermore, LADWP's Water System has a dedicated team to operate and maintain a private water SCADA Network. The goal of this team is to increase operational awareness of network and server activity on a 24 hours, 7 days a week basis to match water operational goals.

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?

LADWP reports to WECC, on matters of reliability standards, and indirectly to NERC and FERC, and to other legislative and regulatory bodies with authorized oversight responsibility for LADWP activity. LADWP receives ES-ISAC information on potential system vulnerabilities.

In the future, LADWP may consider utilizing the Chemical Facilities Anti-Terrorism Standards (CFATS), a set of recommended standards released by the Department of Homeland Security that imposes comprehensive federal security regulations for high-risk chemical facilities.

In essence, LADWP has established policies and procedures to provide all necessary reports to all requesting regulatory agencies per established cybersecurity reporting guidelines.

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

National and International standards and organizations could facilitate the development of sector specific frameworks for organizations that have not already adopted strong cybersecurity programs.

USE OF FRAMEWORKS, STANDARDS, GUIDELINES, AND BEST PRACTICES

1. What additional approaches already exist?

NERC, in its capacity as ERO, has developed as part of its Reliability Standards, a set of CIP Standards, which are mandatory and enforceable for all "users, owners and operators" of the BPS, and hold monetary penalties for non-compliance. The CIP Standards have recently completed their fifth revision, with that revision (Version 5) submitted to FERC for approval on February 1, 2013. According to NERC, the implementation period for this standard will be in approximately two years. Until that time, the prior approved version of the standards are already mandatory and enforceable, as described in the response to question # 7 in the first section of these responses. The ES-ISAC issues alerts to provide actionable intelligence to the industry on cybersecurity threats and vulnerabilities.

NERC, through its Critical Infrastructure Protection Committee (CIPC), also develops voluntary guidance documents, which are used to aid in compliance with the CIP Standards, as well as to address generic security concerns. NERC's CIPC has been developing and modifying guidance documents for more than 10 years, and has recently focused its efforts on providing guidance specific to the Electricity Sub-sector, and providing references to more generic security guidance on its website. CIPC guidance documents include:

- Threat and Incident Reporting
- Threat Alert System
- Physical Security
- Continuity of Business Processes and Operations Operational Functions

The Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) provides a framework for the electricity sector to develop mature cybersecurity programs. Although it was developed for the electricity sector, it could potentially be adopted to other critical sectors' infrastructure.

The NIST Special Publications provide guidelines that are mandatory for federal agencies, but may be used as a guide for implementing best cybersecurity practices for sectors with critical infrastructure.

The International Standards Organization (ISO) 27000 series are a collection of international guidelines developed by the ISO, and contain best practices for the implementation of cybersecurity programs, controls and practices.

2. Which of these approaches apply across sectors?

While NERC's Reliability Standards are specific to the Electricity Sub-sector, many of the concepts are generic, and may be applicable to real-time process control networks and systems in other sectors once proper analysis of the unique attributes associated with risk and the requirements of confidentiality, integrity and availability.

Other approaches as described above on Question #1 may also be used as indicated.

3. Which organizations use these approaches?

NERC Reliability Standards apply to all "users, owners and operators" of the BPS, which is the subset of the Electricity Sub-sector 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."

Please also see response to Question #1 for organizations using and recommending various approaches.

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

NERC Reliability Standards apply to "users, owners and operators" of the Bulk Power System; they do not apply to facilities used in the local distribution of electricity since this is the purview of the State. Further, because the cyber threats are quickly evolving, standards cannot be the whole answer.

Ultimately what is needed is proper threat and vulnerability information to ensure that selected practices and controls are meeting the objective to reduce risk. Furthermore, this actionable, vulnerability information should ensure that organizations can respond to emerging threats, and modify control selections accordingly.

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

Harmonizing different approaches to create one baseline framework that takes into account the NERC CIP standards and guidelines such as the NIST 800-39 is no small feat, but the key will be in properly identifying threats and vulnerabilities, and measuring them against the value of the targets and capabilities of the threat actors.

Another useful tool in existence is the ES-ISAC, which as indicated above, provides actionable intelligence to the electricity sub-sector through alerts. Timely sharing by

the Federal government of actionable information about the threats the electricity industry and other critical infrastructure sectors are facing is critical to that effort.

Recognizing that there may be imminent threats relevant to the energy-sector, at the national security level, a comprehensive approach by the Federal government may be needed to ensure the timely dissemination of that threat information. LADWP generally supports legislation that:

- Preserves the current NERC/FERC process for developing, approving and enforcing cybersecurity standards, as established by the Energy Policy Act of 2005;
- Increases the sharing of timely, actionable information on cyber threats between the Federal government and public and private entities; and
- Grants a single federal agency new limited, emergency power to address imminent cybersecurity threats to the BPS.

The Executive Order 13636 and Presidential Policy Directive 21 take important steps while recognizing that further topics may need to be addressed through legislation.

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

As noted above, the CIP Standards were developed for the electricity sector and applicable to the BPS. NERC follows an ANSI-accredited standards development process, which provides for initial development by industry stakeholders, utilizing their technical expertise, followed by commenting and balloting by interested stakeholders, primarily from the electricity sector. Through this consensus-based process, the standards language is inherently developed to meet the needs and specificity of the members of the electricity sector.

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

NERC Reliability Standards are mandatory and universally applied across all relevant stakeholders within NERC's (and FERC's) jurisdiction. Because NERC Reliability Standards are mandatory and enforceable, users, owners and operators of the BPS do not have any other choice but to comply. In general, sector-specific standards that allow for industry comment and approval ensure majority stakeholder agreement, implementation and willingness to comply.

Because each sector has potentially different threat and vulnerability profiles, the creation of sector-specific voluntary frameworks may be necessary, to ensure that the selection of controls and risk-reduction approaches do not impact the vulnerability of other sectors.

Extreme care must be taken to avoid creation of a second set of potentially conflicting standards.

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 sector coordinating councils (SSC) should focus on emergency support functions, and provide greater focus on distribution and restoration, while leaving standards for the BPS to NERC within its authoritative role. The SSA should work closely with Government Coordinating Councils (GCC) and SCC to facilitate support for the ES-ISACs. The GCC/SCC, along with SSA support, should fully address executive alignment of priorities towards the following:

- Enhanced sharing of timely and actionable threat information
- Enhanced role definition of sector partner organizations
- Enhanced departmental and corporate resourcing and organizational structural alignment and policy for enhanced security dialogue and reporting
- Provision of low cost, high value, pre-event steps using existing constructs
- Programmatic support and resource support for improved cross sector information sharing using the sector ISACs
- Continued support for sector analysis and understanding, as well as capability maturation encouragement
- Achieving leadership consensus across public-private sector partnership which drives emerging policy, implementation guidance, resource adequacy, and role definition

Further, NERC and the Regional Entities should continuously assess the effectiveness of the NERC CIP standards, including whether the standards are not creating unnecessary burdens to the utilities.

9. What other outreach efforts would be helpful?

The SSA and GCC/SCC should be involved in developing and providing executive sponsorship for a collaborative and comprehensive outreach effort, which informs sector participants on key structures, policies, priorities and approaches employed by the sector.

SPECIFIC INDUSTRY PRACTICES

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 above are within the current set of CIP Standards. LADWP employs all of the aforementioned practices in various degrees to secure critical infrastructure and other corporate assets.

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

The new CIP Standards (Version 5) generally cover the same subject areas as both the NIST FISMA framework and the ISA-99 and ISO 27001 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?**

The "separation of business from operational systems" is one of the most critical controls for secure operation of critical infrastructure. Such an approach can greatly reduce the overall "attack surface."

Another related critical practice is to strengthen security without impeding system reliability. If the security framework that is imposed diminishes operability or reduces real-time data situational awareness, operations of the grid can be negatively impacted.

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

All of these practices are applicable and necessary for both business and mission needs.

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

A significant implementation challenge is ensuring that the application of any practice does not impact the reliability of operational systems (control systems, SCADA, etc.), or compromise their protection from untrusted sources.

Another significant implementation challenge within the listed practices above involves "monitoring and incident detection tools and capabilities." Recent events in

multiple sectors have demonstrated that threat actors have significant, technically-capable personnel and sufficient resources to attack and overcome some of the most dedicated security programs in the world. 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 from threat actors is continually evolving with new methods of attack.

The use of encryption and key management on data at rest because of the challenges that present with regard to usability of the data, the productivity of the users, and the performance degradation to the systems. For instance, the SCADA systems have traditionally limited processing speed and memory with sub-millisecond response requirements; the introduction of encryption methods may result in adverse effects to power operations.

Mission/system resiliency practices are a challenge because the cost inherent in fully resilient systems is as much as eight times the cost of a non-resilient system.

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

As noted above, LADWP is required to follow all NERC Reliability Standards, including the CIP Standards. LADWP also follows voluntary guidance developed and issued by NERC and others such as NIST Special Publications, and the International Organization for Standards (ISO).

Additionally, LADWP has created standards and guidelines to address many of these practices, specifically:

a. LADWP maintains a segmented network model such that all control systems are physically separated by firewalls onto isolated networks. Critical Infrastructure Control systems are separated by multiple firewalls administered by IT and Energy Control. This physical separation aligns with the NIST "Separation of business from operational systems" practice.

b. LADWP requires SSL an IPSEC communications between most external entities and LADWP systems. These encryption methods are also utilized on internal core systems to protect them from compromise. Additionally, LADWP wireless network uses various methods for authentication and encryption. These standards align with the "Use of encryption and key management" practice.

c. LADWP has security access and password administration controls which align with the NIST "Identification and authorization of users accessing systems" practice.

d. LADWP maintains an in-house inventory system, and utilizes industry available software to inventory computer systems on the network and to ensure that security patch levels and antivirus signatures are up-to-date. LADWP has software and license management procedures to assist users with software

compliance. These practices meet the requirements of the NIST "Asset identification and management" practice.

e. LADWP employs a variety of network tools including IPS software on the perimeter firewalls and logging and alerting to monitor and detect threats to the network. These practices address NIST's "Monitoring and incident detection tools and capabilities" practice.

f. LADWP complies with all federal and state regulations with regard to privacy and civil liberties. All employee, customer, sensitive, and classified data is managed using information classification and protection procedures, which address NIST's "Privacy and civil liberties protection" practice.

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

LADWP's methodology to properly allocate business resources include the following major activities:

- LADWP conducts an annual review and update of its NERC's cybersecurity policies, procedures, and standards;
- LADWP conducts stringent change and configuration management controls based on proven IT standards as part of ensuring the security, reliability and safety of our systems, and these controls are consistent with NERC CIP standards.
- Additional allocation considerations include workload requirements of the different business units, and audit findings.

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

LADWP, either through a regulatory compliance or information security function, has created an escalation process for cybersecurity risks within the organization.

Additionally, LADWP complies with the CIP standards, which require reporting for significant compliance matters to the ES-ISAC, along with voluntary non-compliance reporting activities. LADWP also conducts vulnerability assessments as required by the CIP standards.

Furthermore, NERC Alerts received by the electricity sector contain the following types of reporting:

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. Action 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?

LADWP is mindful of the legal and regulatory issues surrounding privacy and civil liberties. Those risks may include sharing sensitive information regarding authorization of users accessing systems, and using monitoring and incident detection tools that may expose personally identifiable information if proper safeguards (i.e. encryption) are not integrated, although in the operational infrastructure, the risk is minimal.

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

While LADWP does not have an international footprint, we do have customers living outside the United States with property and power needs located within our retail service area. LADWP is mindful of the confidential nature of our data and inasmuch employs firewall geo-protection and to protect the data from foreign attack.

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

CIP-011 (information protection), within the proposed Version 5 of the CIP standards, discusses handling sensitive information, which can extend to privacy and civil liberties.

Employee, customer, and other confidential data entrusted to LADWP are addressed by the information classification and protection standards created and enforced at LADWP.

Confidential data is protected in transit and at rest. Customers are notified of any change, relocation, or disclosure of their confidential data.

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

Practices addressing the training of staff on protecting sensitive information, and ensuring privacy will help to mitigate any risks to privacy and civil liberty issues.