April 18, 2013

National Institute of Standards and Technology
RE: Request for Information: Developing a Framework to Improve Critical Infrastructure Cybersecurity

All:

UIL Holdings is pleased to submit the attached comments responding to the Request for Information (RFI) that the National Institute of Standards and Technology (NIST) published in the Federal Register on Tuesday, February 26, 2013.

Cybersecurity requires a coordinated effort among companies, the federal government, and the suppliers of critical electric grid systems and components. Electric companies work closely with the North American Electric Reliability Corporation (NERC) and federal agencies to enhance cybersecurity of the power system. This includes coordination with the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE), as well as receiving assistance from federal intelligence and law enforcement agencies.

We encourage NIST to develop a Cybersecurity Framework that provides a high-level and flexible tool for critical infrastructure. In developing this Framework, NIST should consider leveraging existing approaches and public-private cybersecurity partnerships and focusing on cost-effective risk management. We caution against developing new cybersecurity standards because they will likely overlap or duplicate the existing approaches already in use today.

UIL's Responses to NIST RFI Questions

I Current Risk Management Practices

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

   Our greatest challenge is obtaining timely, actionable and currently unavailable cyber threat information. Since the cybersecurity threat environment is constantly changing, the ongoing dissemination of vulnerability and threat information and analysis is needed to inform protective actions. The federal government has considerable knowledge of these cyber threats while electric companies understand the operations of power systems. We need better mechanisms for the government and industry to provide for ongoing consultation, cooperation and the sharing of information with each other to alert companies to potential threats and provide guidance on mitigation of these threats. Such information is important to improving our risk assessment process since it will enable us to focus resources on likely risks.

   Expansion of the Enhanced Cybersecurity Services program to the electricity and Gas sub-sectors is one mechanism with the potential to improve information sharing between the federal government and the electricity and gas sub-sectors. Therefore, we welcome speedy implementation of Section 4 of the Executive Order that directs the government to increase the volume, timeliness and quality of cyber threat information shared with the private sector.

   Supply chain security is also a challenge. The software and hardware components that make up the information and control systems used by industrial control systems are manufactured by a very large number of different vendors, who often are either owned or operated internationally. New vendors and service providers, who may be less familiar with the security requirements and operating environments specific to utilities, are also becoming a part of the sector's supply chain. This complex and dynamic supply chain introduces the risk that flaws or malware can be inserted accidently or intentionally into control system components in a variety of ways.

   Individual companies do not have the resources to assess the supply chain integrity of every component – from millions of lines of software code to thousands of hardware components. However, companies are working with each other, the Federal government, and vendors to reduce the supply chain risk through a number of security efforts including: adoption of secure coding practices, application and component testing, improved procurement language, use of supplier monitoring tools and best practices, and analysis of software and hardware.

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

   One of the key lessons we have learned as we have worked to advance our own readiness is that while standards encourage good business practices and enforce a baseline level of security, standards alone are not sufficient to address cyber threats. Standards take a long time to develop and can provide a road map for our adversaries to evade security controls. It is extremely important to avoid conflicting or unnecessary standards that divert attention from the need for flexibility and creativity in the security context. The establishment of new, or worse, duplicative

standards (even if voluntary) will unnecessarily divert resources and seriously hinder our ability to respond quickly and with agility to real-time cyber threats.

Given this, we believe strongly that the Framework must focus on communications, and existing guidelines and best practices rather than develop or refine detailed standards. The Framework must be flexible, risk-centric, goals-based and process-oriented and avoid an overly prescriptive approach.

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?**

   UIL has a comprehensive set of policy and procedures that govern our control systems. All policies are approved and signed off by the executive sponsor of our program. The Cybersecurity program at UIL has support from the CEO level and on down through the organization.

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

   Within the Information Technology Department

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

   Cybersecurity risk is handled by the manager of cybersecurity. The manager has the support and ability to escalate risk up through the organization and if necessary right up to the CEO.

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

   Cybersecurity is a consideration in all of our organizations decisions.

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

   In addition to the NERC UIL uses:

   - *Electricity Subsector Cybersecurity Risk Management Process* – a cybersecurity risk management guideline developed by DOE, NIST, NERC, and industry subject matter experts;
   - NIST SP 800-30, *Guide for Conducting Risk Assessments*;
   - NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*; and
   - NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

We also benefit from the senior-level NIAC engagement discussed earlier and a host of other information-sharing venues. These include the DHS National Cybersecurity and Communications Integration Center (NCCIC) and the NERC Electricity Sector Information Sharing and Analysis Center (ES ISAC), both of which inform the industry on recommended preventative actions.

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?**

   FERC, NERC, NPCC, DOE

9. **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?**

   The electricity sub-sector is subject to mandatory NERC Critical Infrastructure Protection (CIP) and NRC cybersecurity requirements. Section 215 of the Federal Power Act and FERC gave NERC authority to develop enforceable cybersecurity standards. The NERC CIP-002 through CIP-009 standards were approved by FERC in 2008, making them mandatory for owners and operators of the bulk power system. Since 2008, the standards have been updated as the threat landscape continues to evolve. The NERC CIP standards are tailored to electricity sub-sector cyber risks and focus on protecting Critical Cyber Assets through a number of security practices that support the reliability of the bulk power system. Version 3 is currently used by the electricity sub-sector. Version 4 will replace version 3 on April 1, 2014 and Version 5 was filed with FERC on February 1, 2013.

   In the electricity sub-sector, NERC requires the reporting of reliability disturbances to its Regional Reliability Organization and NERC (Standard EOP-004-1); cyber events to the ES-ISAC (Standard CIP 008-3); and sabotage events to "appropriate systems, governmental agencies, and regulatory bodies" (Standard CIP 001-2). The sector also has reporting requirements to DOE through Form OE-417. Cyber events that interrupt electric system operation must be reported to DOE within an hour of the incident (Emergency Alert). Cyber events that could impact the adequacy or reliability of the electric power system must be reported to DOE within 6 hours of the incident (Normal Alert). DOE reporting is also required within 6 hours if more than 50,000 customers lose electric service for an hour or more and when fuel supply emergencies could impact electric power system adequacy or reliability. Cyber events are also reported to state law enforcement and the FBI for investigation.

   With respect to the ES-ISAC, NERC utilizes an alert system that helps inform electric utilities' response to cyber threats and vulnerabilities. The ES-ISAC developed the following three levels of Alerts to formally notify the industry regarding security issues:

   - Level 1 Industry Advisory – These are purely informational and intended to alert registered entities to issues or potential problems.
   - Level 2 Recommendation to Industry - Recommends specific action by registered entities. Recipients are required to respond as defined in the Alert.
   - Level 3 Essential Action - Identifies actions deemed to be "essential" to bulk power system reliability. Like recommendations, essential actions require recipients to respond as defined in the Alert.

Our industry seeks to have an even better situational awareness of cyber events affecting the government and other sectors of the economy to the extent that these can affect the electricity sub-sector as well. Our industry strongly supports the Executive Order as it seeks to address this need.

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

    On our electric side, our primary communications are owned. On the gas side, we are completely dependent on the Telecommunication carriers.

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

    In our experience every organization operates somewhat differently, but we believe these operational differences are not particularly critical variables in and of themselves. The important thing is that protecting the nation's critical infrastructure is the industry's top priority and assuring cybersecurity and resilience is part of achieving that priority.

    UIL has engaged in multiple discussions of cyber issues and met with various governmental agencies to discuss cyber issues.

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

    The NERC CIP standards and processes apply to the interconnected grid in both Canada and Mexico and are thus international in nature

II Use of Frameworks, Standards, Guidelines, and Best Practices

1. **What additional approaches already exist?**

   NERC/CIP, DOE, TSA, NIST, SANS, DHS

2. **Which of these approaches apply across all sectors?**

   NIST, SANS, DHS

3. **Which organizations use these approaches?**

A number of approaches to cybersecurity already exist for the electricity sub-sector, including mandatory and voluntary standards, frameworks, guidelines and best practices, many of which are discussed below. While standards may have a role in encouraging a baseline level of security and good business practices, standards alone are not sufficient because the cybersecurity environment is constantly changing and evolves rapidly. UIL strongly believes that the NIST Framework should be a

high-level and flexible tool, leverage existing approaches and public-private cybersecurity partnerships and focus on cost-effective risk management. The Framework development process should not try to develop new cybersecurity standards because new standards will likely overlap and duplicate the existing approaches already in use by the electricity and other sectors.

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

   There is a comprehensive array of security frameworks and guidance in place that is able to be leveraged across both our industries. There are few limitations found in them**.**

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

   N/A

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

   Papers published from the TSA and DHS do address sector specific needs.

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

   The nature of a framework should be voluntary. The company should be able to manage and mitigate risk as appropriate for their individual situation.

8. **What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?**

   We are already heavily regulated and controlled by NERC/CIP

9. **What other outreach efforts would be helpful?**

   We have used both the DHS and ES-ISAC outreach programs. They have been informative and unbiased in helping us make good compliance and security decisions.

   <u>Public-Private Coordination Is Required</u>

   Protecting the grid from cyber attacks requires a coordinated effort among electric companies, the federal government, other critical infrastructure sectors the electricity sub-sector depends upon and the suppliers of critical electric grid systems and components. To complement its cybersecurity efforts and to address rapidly changing intelligence on evolving threats, the industry embraces a cooperative relationship with federal authorities to protect against situations that threaten national security or public welfare, and to prioritize the assets which need enhanced security**.** A well-practiced, public-private partnership utilizes all stakeholders' expertise, including the government's ability to provide clear direction and assess threats, while owners and operators of the critical infrastructure develop mitigation strategies that will avoid significant adverse consequences to utility operations or assets.

The NIST Framework should leverage existing public-private partnerships. DHS and sector-specific agencies have worked with the electricity sub-sector during the past decade to improve information sharing, operational resiliency, and emergency response capabilities of critical infrastructure. For example, in 2009, DHS developed the Private Sector Preparedness program (PS-Prep), a voluntary certification program for emergency preparedness.

III Specific Industry Practices

The RFI sought information regarding adoption of the following nine practices:

- **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. General Comments to Answer the Questions about these Practices.

The nine practices listed in the RFI are widely used and are addressed by the NERC CIP standards and the other cybersecurity guidance listed above. The criticality and application of the practice may vary by entity, depending on the operation and information technologies used by an organization's systems and the implementation of these systems. Each poses a unique set of challenges, including implementation, administrative, operational, complexity, and cost. Therefore, a risk management process and a comprehensive strategy incorporating these and other practices for a defense-in-depth approach are needed to address these challenges.

Other practices used by industry include:

- Integration of physical security practices, enterprise IT, and energy control systems
- Robust personnel screening, training and awareness programs
- Threat intelligence and monitoring practices, including information sharing
- Configuration and vulnerability management practices
- Separation of control systems from Internet facing systems
- Removable media control and sanitization
- Change control processes to ensure changes to the IT infrastructure are performed in a controlled and coordinated manner and do not negatively impact cybersecurity
- Procurement protections to ensure products or services of prospective vendors are vetted prior to being approved for use

- Decommissioning practices such as wiping devices/media
- Forensics analysis

Cybersecurity guidance focused on these practices and guided by an organization's risk management process are used for the development of internal cybersecurity policies, standards, and procedures for the protection of IT information and control system assets. During system design, the guidance is used for risk assessment, security by design, and procurement processes. During system operation, the guidance is used for ongoing security efforts, including monitoring, response, and system/asset/user management. As indicated previously, the ES-ISAC provides a three-tiered alert system to the electricity sub-sector that reflects the severity of cyber threats. However, more timely sharing of threat information by the federal government is critical to improve our efforts to identify risks for risk assessment and resource allocation purposes.

2. Privacy

UIL has a long history of protecting the privacy of customer data and respecting the civil liberties of their customers. In view of the development of Smart Grid technologies, the electric industry has had to revisit industry privacy practices and as a result, even stronger privacy standards and practices have been developed, as described below. The electric industry continues to work with federal and state officials (including NIST), as well as other stakeholders to refine and improve its privacy standards and practices.

Answers to Questions regarding Privacy

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

Protecting customer privacy is an important and well-established priority, virtually all of whom have policies in place to protect access to customer data**.** Traditionally, privacy regulation of customer data has been the responsibility of the states, and virtually all of the states have developed various data privacy, access and disclosure laws governing utility customers. States and the federal government also have consumer protection laws safeguarding the interests of energy consumers.

The deployment of Smart Grid technology has introduced new data collection and information sharing abilities related to customer data, and in recognition of the privacy and data access issues which have been raised, electric utilities have acted in coordination with state and federal officials (including NIST), stakeholders and privacy experts to update their policies and procedures. Generally, these updated standards and practices are based on Fair Information Practice Principles ("FIPPs"), such as those outlined in the White House Report entitled "Consumer Data Privacy in a Networked World" and the Federal Trade Commission ("FTC") report entitled "Protecting Consumer Privacy in an Era of Rapid Change." Another example of a recent industry standard is NAESB REQ.22, which establishes voluntary Model Business Practices for Third Party access to Smart Meter-based information. Similarly, Volume 3 ("Privacy and the Smart Grid") of NISTIR 7628 provides another example of updated industry guidelines/recommendations based on FIPPs principles. The NIST Cybersecurity Working Group ("NIST/CSWG") continues its work in this area through its Privacy Subgroup. More recently, the industry has been working with the Department of Energy ("DOE") to develop a voluntary code of conduct ("VCC") consisting of the following elements:

- Management and Accountability;
- Notice and Purpose, Choice and Consent;
- Use and Retention; Individual Access;
- Disclosure and Limitations;
- Security and Safeguards;
- Accuracy and Quality;
- Openness, Monitoring, and Challenging Compliance; and
- Enforcement Mechanisms.

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

As noted above, the aforementioned standards and practices are based on FIPPs that are internationally recognized. The Organization for Economic Co-operation and Development ("OECD") Privacy Principles represent an example of similar principles. Internationally, the OECD Privacy Principles provide the most commonly used privacy framework. Existing and emerging privacy and data protection laws reflect OECD Privacy Principles, which continue to serve as a basis for the creation of leading practice privacy programs and additional principles.

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

Standards or guidelines of the kinds identified above provide useful references in assessing the adequacy of existing policies and practices, and updating them where needed.

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

The primary privacy issue related to the deployment of Smart Grid technologies is that the collection, transmittal and maintenance of personally identifiable data related to the nature and frequency of personal energy consumption and production in a more granular form. However, the privacy practices already in place have not proven to be a threat to civil liberties, but rather reflect industry commitment to protect customer privacy.

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

Risks to privacy and civil liberties in the utility industry should continue to be managed through the implementation and refinement of existing privacy practices and principles.