Response to NIST RFI – “Developing a Framework to Improve Critical Infrastructure Cybersecurity”, (Docket # 130208119–3119–01)

April 08, 2013

JEA

ATTN: COMPLIANCE & RISK
21 W CHURCH ST.
JACKSONVILLE, FL 32202-3155
www.jea.com

JEA sm

Building Community sm

Table of Contents Page

1.0 Background 3

2.0 About JEA 3

3.0 For Further Information Contact 4

4.0 Section 1: Current Risk Management Practices 4

5.0 Section 2: Use of Frameworks, Standards, Guidelines, and Best Practices 12

6.0 Section 3: Specific Industry Practices 15

7.0 JEA's Recommendations 19

7.1 Vendor Compliance with Standards and Framework 19

7.2 Consideration of existing Cyber Security Standards 19

7.3 Avoidance of Unnecessary Overhead 19

7.4 Utilize the results of existing projects in the field 19

7.5 Consideration of Induced Risk on Critical Infrastructure 20

8.0 Appendix – Referenced Resources 21

1.0 Background

Under Executive Order 13636 ("Executive Order"), the Secretary of Commerce is tasked to direct the Director of NIST to develop a framework for reducing cyber risks to critical infrastructure (the "Cybersecurity Framework" or "Framework"). In order to accomplish above objectives, the National Institute of Standards and Technology (NIST) is conducting a comprehensive review to develop a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework" or "Framework"). The Framework will consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

This notice for Request for Information (RFI) published on NIST website on February 26, 2013, requests information to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop the Framework. For the purposes of this RFI, the term "critical infrastructure" has the meaning given the term in 42 U.S.C. 5195c(e), "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The NIST RFI notice states that comments must be received by 5:00 p.m. Eastern time on Monday, April 8, 2013.

JEA is a member of two of twelve identified Critical Infrastructure sectors, *electric and water*. JEA is submitting this response to the RFI, as it strongly believes that a cross-sector standards-based cybersecurity risk Framework can provide substantial benefits to all the sectors by standardizing and streamlining the risk evaluation process, improve technology delivery from vendors that support these sectors, help early detection, and streamline coordinated response to newly emerging threats. Such a framework when applied effectively across sectors can also enhance inter-sector coordination for improving security preparedness and limit risk dissipation between the industries where these sectors are linked and dependent on shared services. JEA sincerely hopes that business drivers, operating environment diversity and technical delivery platform limitations are given sufficient importance in development of such framework.

2.0 About JEA

JEA, located in Jacksonville, Florida, is a not-for-profit, community-owned utility that serves an estimated 420,000 electric, 305,000 water and 230,000 sewer customers in Northeast Florida. JEA owns and operates six generating facilities including two small methane-fueled generating units.   JEA is a joint owner of two other generating facilities. The total generating capacity is approximately 3,757 megawatts. JEA owns transmission and distribution facilities including 729 miles of transmission lines and 6,547 miles of distribution lines.

JEA's water and wastewater operation consists of 136 artesian wells tapping the Floridan aquifer, which is one of the world's most productive aquifers. Water is distributed through 36 water treatment plants and 4,208 miles of water lines. More than 3,760 miles of collection lines and seven regional and seven non-regional sewer treatment plants comprise the JEA sewer system.

The primary purpose of JEA's business is to provide reliable services at a good value to our customers while ensuring protection of our natural resources. JEA is a member of the American Public Power Association

(APPA) and the Large Public Power Council (LPPC) and supports the comments submitted to you by those entities.

3.0 For Further Information Contact

<u>Primary</u> –

Daniel D. Mishra
Director – Critical Infrastructure Protection (CIP) Compliance
JEA, (7th Floor, JEA Tower)
21 West Church Street, Jacksonville, FL- 32202
Office: (904) 665-7655 | Fax: 904-665-6335

<u>Alternate</u> –

Ted Hobson
Chief Risk & Compliance Officer
JEA, (16th Floor, JEA Tower)
21 West Church Street, Jacksonville, FL- 32202
Office: (904) 665-7126 | Fax: 904-665-4238

4.0 Section 1: Current Risk Management Practices

NIST is soliciting 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?**

JEA sees many challenges to the effective application of cybersecurity practices across critical infrastructure. The following observations highlight some of the key challenges.

a. **Vendor products and support practices often do not conform to risk frameworks and compliance standards –** Without publicly divulging details or naming specific vendors, it is important to recognize that many of the control systems in SCADA and DCS environments lack security controls that meet the needs of today's cyber-secure environments. The NIST Risk Framework should propose that vendors must design and develop products with the risk framework in mind, and that vendors adequately support upgrades to legacy systems, where technically feasible.

b. **Overly-broad information sharing restrictions –** Often, the restrictions on the sharing of information possessed by governmental agencies impose a barrier to effective cybersecurity prevention and mitigation. Even when all stakeholders have good intent, restrictions on information disclosure in existing standards or statutes may overly limit or restrict the sharing of relevant information that could be declassified, but remains classified. It is important to note that otherwise "high value" information that may be useful in detecting and preventing cybersecurity threats is essentially "worthless" if preventative measures are not timely disclosed to owners and operators of critical infrastructure. All efforts should be made in the NIST framework to provide relevant threat prevention information (in declassified form) to the personnel who will apply such information in defensive measures to protect critical infrastructure from emerging malicious attacks.

c. **Rapid changes to the threat paradigm –** The rate of proliferation of cyber threats against critical infrastructures appears to be increasing, and this increasing rate of proliferation may further accelerate. As nation states, organized groups, and individuals (both international and domestic) find sufficient sponsors to fund the discovery and exploitation of vulnerabilities in the critical infrastructure for offensive uses, it is essential that as a nation we are able to share our combined knowledge and leverage both public and private resources to create an effective defensive protocol to thwart any such threats.

d. **Operational limitations –** Unlike redundant IT infrastructure, the reliability uptime and specialized nature of SCADA and DCS systems create potential problems for patch management regimes that rely on frequent reboots or firmware upgrades. In post-Stuxnet world, where nation states are developing offensive cyber warriors, SCADA and ICS researchers and academics are now making public disclosures of vulnerabilities (even before fixes are developed) instead of only reporting such vulnerabilities to vendors and government agencies. Such developments have placed the SCADA and ICS environment at risk. JEA highly recommends that NIST should propose alternate approaches to handling such emerging risks and impress upon SCADA vendors to devise built in counter measures for new emerging threats such as Stuxnet.

e. **Competition for resources –** Obscurity has been a protective measure for the electric critical infrastructure for quite some time, but recent integration and merger of technologies has exposed electric infrastructure to vulnerabilities. However, resources to improve the security defenses of critical electric infrastructure are generally scarce, and must be coordinated with the operational characteristics of the facilities. There are very few qualified specialists who understand both the operational characteristics and security needs of critical electric infrastructure. It is important for reliable and secure critical infrastructure to train and maintain a qualified cybersecurity workforce.

f. **The NERC and FERC zero-tolerance CIP enforcement framework is not optimal for security –** NERC and FERC have chosen to adopt what has become essentially a zero-defect enforcement paradigm wherein entities face the risk of financial penalties for every minor mistake, even for self-reported corrections, and even for events with negligible impact to reliable operations or cybersecurity. Such a least-common denominator approach diverts scarce resources to paperwork and "check-the-box" type tasks that document compliance. And such resources are then not available for other reliability and/or security improvements. The current system is also plagued with long delays in drafting and approval of new and revised standards, as FERC, NERC and stakeholders are fixated on the precision and correct wording of the standards, rather than the "intent" of the standard. Such delays slow reliability responses and retard implementation of improvements. The Framework must avoid such pitfalls and focus on a program that provides guidance on risk mitigation, monitoring of effective implementation and correction of risks as they are identified by assessments. Penalties and enforcement actions should be limited to conditions that deserve such an action such as dereliction of responsibilities, intentional avoidance of risk mitigation for financial gains, lack of compliance program or a compliance program fraught with ineffective controls.

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

JEA sees many challenges in developing a cross-sector standards-based Framework for critical infrastructure.

a. **Systems diversity and distinctness.** – Systems and devices that are designed with different environments in mind may have difficulty conforming to a single cybersecurity framework. For example, a device that is designed to be connected to the top of an electric pole, often does not envision a security threat as one of the key risks, but rather focuses on placement, accessibility, operating field environment conditions, and connectivity as key attributes.
b. **Divergent modeling priorities.** – Certain sectors may adopt a modeling priority of Confidentiality-Integrity-Availability, while other critical infrastructure sectors may prioritize the modeling framework as Availability-Integrity-Confidentiality. Such distinct modeling priorities have led to differences in system security design. It may prove difficult to design a single framework that can incorporate divergent virtues and differing priorities.

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?**

JEA, similar to most organizations, views risk as anything that has the potential to disrupt delivery of service, affect quality of service, or result in a failure to meet organizational objectives, the impact of which could be limited or avoided through preemptive actions. Cybersecurity risk is defined as failure of Cyber Assets to perform their designed purpose, resulting from exploitation of any vulnerability or defect by external or internal factors.

JEA's cybersecurity risk management approach is to prioritize risks based on the potential impact to

JEA's strategic objectives. The reliable operation of the BES is the core objective along with providing safe and secure delivery of service to our customers and community.

JEA has policies and procedures for governing cybersecurity risk and our senior management (Chief Risk & Compliance Officer and Chief Information Officer) are actively involved in the governance process. Such a process includes periodic reports (risk index, risk assessments and evaluation, and internal compliance assessments, and external audit reports), mitigation sign-offs, incident reports and steering committee updates. JEA is also involved in a continuous learning enterprise. JEA has documented internal controls that include corrective measures to improve upon its policies and procedures through regular reviews, and when incidents do occur, JEA conducts thorough incident responses with the objective of strengthening its reliability controls to prevention reoccurrences.

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

Some organizations locate their cyber security risk management program under a Chief Information Officer, as all control implementation responsibility is maintained under this portfolio. In this design, however, with the assessment and governance of risk located under the Chief Compliance Officer, whose portfolio usually also includes oversight of security controls, two functions must work in tandem, and independent monitoring of effective cybersecurity risk management controls may be lacking. In contrast, JEA has designed its cybersecurity risk management program to provide both effective implementation and independent oversight of internal controls. Under JEA's current program, responsibilities are assigned to separate executive personnel, a Chief Compliance Officer and a Chief Information Officer.

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

Please refer to our response to question 3 of this section.

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

JEA views cyber security risk as any applicable cyber vulnerability that can be exploited or lack of control of technology system asset operations, information or service that has the potential to disrupt delivery of service or result in a failure to meet organizational objectives.

JEA has risk indicators to help plan, assess, control, contain and mitigate cyber security risk for the enterprise as whole. Senior management is directly involved and often reviews the reports on the activity. The corporate funding process considers these risk indicators as essential for annual planning and such consideration plays a major role in JEA's long term enterprise planning. For most of the organization, JEA has created a risk monitoring matrix, where impact and probability are key factors. For the balance of the organization, objectives are based on this risk index and application of cybersecurity controls is assessed based on objective analysis.

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

JEA's practices can be segmented in two different groups. For the BES operation, JEA strictly applies the NERC CIP standards. For the electric Critical Infrastructure, JEA has established a separate department, Critical Infrastructure Protection (CIP) compliance, responsible for assessing, educating, monitoring and mitigating any identifiable cyber security risk, direct or indirect, that impacts the security or reliable operations of JEA's electric operation. Implementations of controls are continuously monitored using internally developed tools, and external reporting tools required by the FERC approved Compliance Monitoring and Enforcement Program (CMEP). JEA's senior executive management is provided regular updates and stays actively involved by being part of CIP Steering Committee. Other committees are designed to engage critical stakeholders at various levels. JEA has established an Internal Compliance Program (ICP) for monitoring all NERC Reliability standards including the cybersecurity standards. This group is independent of the system /control owners influence and reports directly to the Chief Risk and Compliance Officer (CCO).

For balance of the JEA operations, subject matter experts often depend on approaches that are industry best practices, NIST guidelines, successfully implemented by peers or recommended by consultants. Such practices and tools are customized to meet JEA operational needs. JEA's internal risk assessment departments evaluate the risk and quantify them based on impact and threat/probability. JEA cybersecurity risk management activities are aligned to address the management priorities set based on the annual risk evaluation.

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?**

For its electric side (Bulk Electric System assets) of the operation, JEA 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 Section 215 of 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 electric grid. Of the twelve critical infrastructure sectors designated by the Department of Presidential Policy Directive 21, the electric industry is the only one with mandatory enforceable CIP Standards.

The CIP standards establish a baseline level of security requirements for generation, transmission and control system assets. The CIP standards cover topics such as: Critical Cyber Asset Identification, Security Management Controls, Cyber Security – Personnel and Training, Electronic Security Perimeters, Physical Security of Critical Cyber Assets, System Security Management, Incident Reporting and Response Planning and Recovery Plans for Critical Cyber Assets, among other matters. JEA and other utilities with CIP compliance responsibilities are audited regularly and have continuing obligations for cyber and physical security compliance.

JEA has to demonstrate compliance with all the CIP standards at all times as these standards are zero risk tolerance. JEA's compliance is regularly monitored by an independent body of auditors also referred as the Compliance Enforcement Authority (CEA). CEA operates under authority of Congress and designation by the FERC, and uses eight different mechanisms to monitor and assess JEA's compliance with CIP standards. JEA is required to self-certify compliance every year. JEA is audited for full compliance with CIP standards on a three year cycle, with additional Spot-Checks of compliance with a subset of CIP standards.

For the balance of the organization (including, Water and Sewer operations not subject to mandatory reliability standards), JEA continually strives to maintain high security standards that are guided by principles of risk, safety and quality service to the customers and community we serve. JEA on a regular basis, assesses the risk, designs additional controls and technology improvement projects to improve cyber security in these non-regulated areas of the operation. These controls are internally monitored and assessed, and independently verified by external auditors.

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

All essential data communication functions of JEA's critical assets (inferred from Critical Infrastructure) are independent of the other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors. This independence is by design to provide JEA critical assets with discrete control and monitoring of the BES operations at all times through a secured separated network. This design allows JEA to securely and safely transfer data quickly on these private channels thus limiting any delay to the control signal which can have serious debilitating effect on the performance of BES control systems.

JEA owns and operates electric and water infrastructure and is responsible for Electricity Sub-sector, industrial control systems, energy market systems, energy management systems, and various energy generation, transmission, and distribution systems. Voice communication is essential for reliable operation of these critical assets and lack of reliable telecommunication service can have some impact on the JEA operations. JEA maintains multiple alternatives (redundant) for communicating with other utilities that we partner with and are dependent on, for providing a reliable service to our customers and the community.

However, some of our less essential functions that involve sharing data with other dependent utilities and reliability coordinators do involve use of the commercial telecommunications network. JEA has made efforts to maintain redundant channels of communication and often we subscribe to multiple service providers. JEA presently has very limited dependence on the other infrastructures such as financial services, and transportation sectors, although increasing dependence over a very long time horizon is possible.

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

Managing cybersecurity risk is a key performance indicator for JEA and risk is tracked and monitored at various management levels. Operational objectives are given the same emphasis as the cybersecurity goals unless they are influenced by emergency conditions. Stakeholder safety, security, sustainable and uninterrupted operation are key performance goals for JEA for delivery of services. User perspective is often considered and their priorities are objectively analyzed but security is not forsaken for convenience.

For Critical Electric Infrastructure, NERC CIP cybersecurity standards are mandatory and carry a punitive penalty structure for non-compliance. JEA has to comply with these standards at all times. NERC and FERC have adopted what amounts to a "Zero" defect approach to reliability compliance enforcement. While the rationale behind such an approach is well understood, the consequences of such a rigid "check-the-box" approach to reliability that focuses intensely on compliance documentation has unintended negative consequences for reliability and security. Unfortunately, another consequence of the present NERC and FERC reliability compliance regime are long and cumbersome processes to create new or revised reliability standards. The registered entities have incentive to evaluate and contest every word included in the draft standards, because under the strict liability approach adopted by NERC and FERC, an incorrect interpretation of a single word or comma may adversely impact the entity. Further, such a misguided least-common denominator approach to reliability discourages continuous reliability improvement and dilutes the true intent of the reliability risk reduction framework.

JEA recommends that the NIST framework should propose an approach to cybersecurity risk assessment and standards development that is not complicated by considerations of regulatory enforcement. Such an approach will lead to faster adaptation of the standards as stakeholders will target the objective of the cybersecurity standard and intended risk mitigation. Standard's success will be gauged by the mitigation of security risk not the underlying discussions around the grammatical meaning of the words comprising the standards. Such an approach should prioritize rapid sharing of best practices and foster continuous learning, and avoid diverting scarce resources to "check-the-box" compliance paperwork that does not further reliability or security objectives.

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?

JEA as an electric sector participant is registered for multiple functions based on our operating responsibility to the BES. JEA reports to many regulatory agencies based on their delegation agreements and the authority assigned to them by FERC.

CEA – Compliance Enforcement Authority (CEA) is the regional organization with authority delegation from FERC for monitoring and enforcement of NERC reliability standards. Florida Reliability Coordinating Council (FRCC) based in Tampa, Florida is the regional CEA for the Florida region. As stated in response to question 8 of this section, JEA complies with all reporting requirements as requested by the regional CEA. JEA's experience has been very satisfactory as CEA are represented by a very capable and experienced work force that monitors compliance. They perform such role in an independent manner, but at the same time, CEA staff is eager to discuss situations, agree to mitigation measures and partner in all reliability matters as needed.

NERC – The North American Electric Reliability Corporation's (NERC) mission is to ensure the reliability of the North American bulk electric system. NERC is the electric reliability organization (ERO) certified by the FERC to establish and enforce reliability standards for the bulk electric system. NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast, and summer and winter forecasts; monitors the bulk electric system; and educates, trains and certifies industry personnel.

JEA as a member of this organization is responsible for reporting all the data requested by NERC from time to time. NERC also issues Cyber Security advisories and alerts when any credible vulnerability is recognized or discovered. JEA has the responsibility to abide by the guidance given by the NERC advisories and take precautionary and preventive measures. JEA also has to respond to these alerts/advisories and submit reports if necessary or required by NERC.

ES-ISAC – The Electricity Sector Information Sharing and Analysis Center (ES-ISAC) shares critical information with industry participants regarding infrastructure protection. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other ISACs about threat indications, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning.

JEA is required to report certain Cyber Security Incidents mandated by CIP standards to the ES-ISAC. ES-ISAC has a very supporting role and often engages entities by sharing knowledge of their outward facing network, any known and visible vulnerabilities. ES-ISAC is also responsible for sharing lessons learned from other cyber security incidents reported to them. ES-ISAC serves the electric sector by disseminating threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants in taking protective actions.

FERC – The Commission has concurrent statutory jurisdiction over reliability compliance under Section 215 of the FPA, and it closely oversees the actions of NERC to enforce compliance with statutory enforced CIP standards under the NERC and regional delegation agreements such as the ones incorporated with NERC and FRCC. These regional entities monitor compliance and assess cyber security risk on behalf of FERC. Recently, FERC has also executed its separate jurisdictional authority to directly review and assess compliance with the CIP standards.

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/international standards and organizations that develop national/international standards need to be actively involved in critical infrastructure cybersecurity conformity assessment in order to meet the objective of designing comprehensive and complete cyber security standards. In order to improve their effectiveness, such organizations need better understanding of the infrastructure operations, its business drivers, service delivery methods and limitations. Such factors also play a key role in an organization's ability to conform to the standards. If the primary focus is on assessing the threats, vulnerabilities, and the potential impact of such threats, it is possible to overlook effective countermeasures and security options inherent in the operational characteristics of the critical infrastructure.

Further, organizations are multi-faceted in their operations and often objectives and dependencies overlap among all participants. For example, JEA as an electric sector participant has significant dependence on telecommunications and finance sectors for meeting its business objectives. Cyber security risk, which is often drawn by impact to its objectives, can use common assessment criteria, resulting in a more effective and streamlined process utilized across the organization. However, implementation recommendations should be based on separate assessments of the overall effectiveness to the organization. Priorities of organizations with different sector participation will vary considerably and so will the resources available to different organization. Standards should be tailored to such differences and should allow flexibility for addressing cyber security risk based on the services performed and the resources available to the subject organization.

While technology and emerging threats are dynamic in nature, standards development and the ES-ISAC provide key tools to address new threats and vulnerabilities for the Electricity Sub-sector. However, it is incumbent upon NERC and similar organizations to improve the standards developments process and the quality of deliverables. Such standards should be appropriate, timely, and provide clear and precise objectives. Above all, they should never lead to any confusion.
The standards development process should also consider the need for addressing threats and vulnerabilities that are not directly addressed by the enforced standards, so that in absence of an approved standard, organizations are obligated to mitigate new and emerging threats.

5.0 Section 2: 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 PUCs; 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.

1. What additional approaches already exist?

ISO-27001 – For Information system functional and operational risk assessment, JEA understands that ISO-27001 is a common framework utilized across many sectors. ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control. The key benefits of 27001 are:

- It can act as the extension of the current quality system to include security
- It provides an opportunity to identify and manage risks to key information and systems assets
- Allows an independent review and assurance on information security practices

Cross sector application of ISO-27001 is quite effective because it is suitable for protecting critical and sensitive information and provides a holistic, risked-based approach to secure information and compliance. Application of ISO-27001 in an Information Systems organization demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.

However, for Industrial Control Systems (ICS), ISO-27001 systems application has to be managed in a manner so that limitation of ICS systems are given due consideration. ICS systems prioritize availability at a higher degree than integrity and confidentiality.

NIST 800-82 (ICS), NISTR 7628 and NIST Smart grid Framework 2.0 – JEA has reviewed many of NIST publications that have a wealth of cybersecurity framework specifications well documented and feels that with minor cultivation, this publication can be an ideal starting point for finalizing the cybersecurity framework.

2. Which of these approaches apply across sectors?

HIPPA and PII practices are often applicable across sectors. However, NERC CIP, can be modified to address the cyber security risk in other sectors as well.

For the Smart grid, JEA has elected to use the C2M2 (DOE Cybersecurity capability maturity model) to address the cyber security risk to its Advanced Metering Infrastructure (AMI).

3. Which organizations use these approaches?

NERC CIP is mandatory for NERC-registered entities in the electric sector based on functional classification, and most organizations that own or operate facilities defined as part of the BES in the continental United States have to apply and comply with the CIP requirements. For all other approaches, JEA is not in the best position to respond to this question.

Within JEA, risk assessment methodology is applied based on asset risk portfolio. An asset with personnel identifiable information is assessed against PII and a BES asset is assessed against CIP-002 (Risk Assessment Methodology).

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

NERC CIP is a sector specific approach and covers only certain defined facilities that have a high risk to the reliable operation of the BES. The application of CIP bright-line risk thresholds based on facility operational characteristics to designate Critical Assets and Critical Cyber Assets may not be conducive for broadly limiting cyber security risk. Malicious attackers can induce equal or greater potential damage to utility operations by attacking multiple smaller assets, if such assets are left unprotected.

A comprehensive approach should address all interconnected assets, based on the risks and their operational priorities and integration limitations. Only an approach such as this will truly result in the defense-in-depth solution for the BES.

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

In order to make these approaches more useful across all sectors, NIST should employ a more consultative approach to development; provide use test case scenarios for applicability or lack thereof. It is important to partner with the industry during the development and the implementation, create risk mitigation and consulting services center at all the sector specific agencies. Developing a qualified educational module with certification credential may also be helpful to the industry.

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

In order to account for sector specific needs, most approaches are formulated to be generic in nature. ISO-27001 is generic enough to be applicable to all sectors. However, degree of effectiveness in limiting the cybersecurity may vary.

On the other hand NERC CIP standards were developed by, and for the use of, the Electricity Sub-sector. 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 Sub-sector. Through this consensus-based process, the standards language is inherently developed to meet the needs and specificity of the members of the Electricity Sub-sector.

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

Both methods are appropriate, but care must be taken to ensure they work together. NERC Reliability Standards are mandatory and generally applied across all relevant stakeholders within NERC's (and FERC's) jurisdiction. They provide the baseline framework upon which all other standards and guidance statements are layered. Because NERC Reliability Standards are mandatory and enforceable, users, owners and operators of the bulk electric system do not have a choice about whether to follow them. 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?

Sector Specific Agencies (SSA) should align departmental priorities and resourcing towards leveraging existing frameworks after gaps are identified and ensure that gaps and vulnerability information is shared in an effective manner that leads to no confusion. The SSA should work closely with Government Coordinating Council and Sector Coordinating Council to facilitate support for the ISACs. SSA 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

9. What other outreach efforts would be helpful?

JEA agrees that a comprehensive outreach effort, which informs sector participants on risk assessment framework structures, policies, priorities and approaches employed by the sectors and illustrations by providing sector specific examples will be very helpful. JEA recommends that educational seminars, training workshops, online as well as computer based training materials methods be used. JEA highly recommends that onsite training be another avenue that should be researched and if that is not as effective, test case/use case scenarios be employed for training the stakeholders.

6.0 Section 3: 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?

Most of the practices mentioned above are addressed in the current NERC CIP standard to a varying degree. Some practices such as use of encryption and key management; security engineering practices; and privacy and civil liberties protection are not included in the NERC CIP standard. NERC CIP standards are designed for electric sector and often not well designed to combat emerging threats. It is important that standards are clear and consistent and address the root causes of cybersecurity risk.

JEA believes that involvement of NIST and other standards development organizations will positively influence and support the maturity of the NERC CIP standards development process.

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 Standards, along with the standards that they also reference. CIP Version 5 includes NIST Framework concepts such as:

- Ensuring that all BES Cyber Systems associated with the BES, based on their function, receive some level of protection;
- Using a tiered approach to security controls, which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the BES;
- Tailoring protection to the mission and operating environment of the cyber systems subject to protection;
- The concept of the BES Cyber System, and
- The inclusion of "Assess" and "Monitor" steps by adding requirement language for "identifying, assessing, and correcting" deficiencies in controls as part of the requirements' expected performance.

The NERC CIP Standards have been mapped against the existing NIST framework, as expressed in SP800-53; the technical requirements of both sets of standards address the same areas. One example of a mapping document was performed by the Control Systems Security Program of DHS in 2009. The area where the SP800-53 control statements do not overlap are in the reporting and administrative areas (e.g., certification and accreditation), which are not required in the civilian private sector. NERC Reliability Standards generally address these areas via its compliance and audit program.

NERC Reliability Standards are mandatory and enforceable for affected registered entities within the continental United States. If a requirement does not otherwise contain any qualification or exemption language, the requirement must be implemented as written in all cases, on all applicable systems, and is subject to a compliance and audit process. Guidance documents and voluntary standards, such as existing NIST and international standards, do not have these restrictions, and are therefore free to provide suggested implementation language within them.

NERC Reliability Standards are generally written as strict liability performance standards – that is, they prescribe an end-state goal that can be measured, and attempt to not specify a technology or method for attaining that goal, and are generally interpreted rigidly without assessment of intent. The CIP standards have evolved in this practice during their development, and the Version 5 standards represent the latest step in that evolution.

An example of this process and evolution can be found in the anti-malware requirements. CIP Versions 1.0 through 4.0 requires anti-malware software to be running on all computer systems within a protected boundary, or else have a documented and approved exception to the requirement. Under the compliance process, even network switches qualify as computer systems that must run the anti-malware software, even though all agree that commercial anti-malware software is not available for network switches. Under Version 5, the anti-malware issues were re-cast as a higher level preventative goal-oriented requirement (i.e., "deploy methods to deter, detect or prevent malicious code" and "mitigate the threat of detected malicious code") rather than requiring anti-malware software running on every computer system within the boundary.

However, there is still some more effort needed to improve the structure and application of NERC CIP standards. JEA is quite optimistic that the NIST framework will provide a spark to restructure the NERC and FERC compliance processes toward true reliability improvements by identifying gaps and supporting the electric sector in mitigating the identified gaps.

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

JEA believes that the following practices as being the most critical for the secure operation of critical infrastructure –

- Asset identification and management;
- Identification and authorization of users accessing systems;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Security engineering practices;
- Mission/system resiliency practices;

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

It is to JEA's understanding that all the practices listed above are applicable and to some degree higher than others. However, focus on these practices varies based on entity size and risk tolerance.

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

The most significant implementation challenge within the bulk electric system is ensuring that entities adequately protect their operational systems (control systems, SCADA, etc.) from untrusted sources. While JEA strives to maintain a very secure environment, proliferation of cybersecurity risk exist from external connections to the ICS environment. ICS environment has sufficient dependency and connectivity to support and product vendors. JEA recommends that NIST should propose minimum cybersecurity protection guidelines for these environments that are external to Critical Infrastructure and maintains network connectivity.

The use of interoperable operating systems and networks has introduced a variety of threats and vulnerabilities to control system environments. While the NERC standards require protections to be in place to secure SCADA systems, these networks are becoming more reliant on connections to third parties, such as other corporate business systems, other electric power entities or system vendors. Thus, simply segregating SCADA systems from a company's corporate networks is not sufficient. This is why NERC and ES-ISAC perform many other activities outside of standards and enforcement to provide the industry awareness and education on the dynamic risks inherent to the sector. JEA recommends that such collaboration between sector-partners should be encourages and documented in the framework.

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

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 threat vectors have changed and the electric sector has gained sufficient attention.

Advanced Persistent Threats (APT) sources have significant, technically-capable personnel and sufficient resources to attack. However, JEA and most of other utilities, defense against APT attacks is often at the other end of the scale in terms of personnel and resources, both in-house and through third parties.

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

Methodology practices vary in rigor and scope with the most vital Electricity Sub-sector environments having stringent change and configuration management controls based on proven IT standards as part of ensuring commitment to reliability and safety, including enforced NERC CIP standards.

All Electricity Sub-sector participants that are NERC-registered users, owners and operators of the BES are required to follow the applicable NERC Reliability Standards, including the Critical Infrastructure Protection standards.

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

JEA subscribes to various CERT advisories and incorporates the required escalation plan to address cybersecurity risks that suddenly increase in severity. JEA also has incorporated a process for evaluating risk and evaluations are conducted annually.

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

Risks to privacy from application of these practices may include sharing sensitive information regarding authorization of users accessing systems. If individuals' names are tied to the authorizations that may raise privacy and civil liberties concerns, particularly if a data breach occurs.

Internal monitoring, if implemented incorrectly, may also infringe on privacy and civil liberties of employees and other stakeholders. Policies and procedures can be adopted to ensure that such privacy and civil liberties safeguards are strictly maintained.

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

JEA, located in Jacksonville, Florida, is a not-for-profit, community-owned utility that serves the limited operational area of Jacksonville. Accordingly, JEA does not envision international implications of this framework on its business or in policymaking in other countries.

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

JEA recommends that risks to privacy and civil liberties safeguards be managed with appropriate safeguards, while continuing to give operational and cybersecurity risk precedence in areas where conflict may occur. Provisions for conflict resolution and a recommended approach for resolution should be outlined by NIST in the framework.

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

JEA believes that NIST Framework should also adopt core practices to protect from disclosure information that relates to Critical Infrastructure. Many entities are governed by State freedom of information laws (Florida Sunshine) which may limit the control of such information. State laws that broadly require information related to Critical Infrastructure to be made available to the public will adversely affect efforts to combat cybersecurity threats.

7.0 JEA's Recommendations

7.1 Vendor Compliance with Standards and Framework

JEA recommends that NIST framework should recognize product and service vendor's essential contribution to the cybersecurity of the critical infrastructure. If vendors are not subject to conformance to with cybersecurity standards and the new NIST framework, all those owners and operators of critical infrastructure who rely on vendor products and support will be limit in their ability to comply and to implement security improvements. The NIST framework should consider this possible limitation and the critical role of vendors and require certification of vendor conformance to the NIST framework. Such approach can be implemented by vendors certifying product or service conformance or through other accreditation organizations such as ISO or ISACA.

7.2 Consideration of existing Cyber Security Standards

NERC CIP mandatory compliance cybersecurity standards went in effect in 2008 after they were approved by FERC. JEA, as an electric utility, has invested considerable resources in complying with the letter of the NERC CIP framework. It would be counterproductive if the new NIST risk framework resulted in competing compliance or audit regime that subjected NERC-registered entities to conflicting or overlapping responsibilities. JEA encourages NIST to avoid imposing additional requirements on NERC-registered entities that would require that they demonstrate compliance to multiple agencies. Instead, JEA urges NIST to heavily weight the preference of using existing regulatory structures before recommending that any additional regulatory agency assume governance or oversight responsibility.

JEA's agrees with the approach that NIST framework should identify or should have provisions to identify gaps in the current regulatory structure. As required by Section 10 of the Executive Order, it is incumbent upon the subject regulatory agencies to correct the identified gaps in the regulatory standards.

7.3 Avoidance of Unnecessary Overhead

The NIST risk framework should have the primary objective of assessment and control of cybersecurity risk. If the risk is not applicable or is negligible to any given environment, entities should not be burdened with documentary paperwork burdens to document compliance activities. Such overhead burdens should be minimized, and limited to areas of greatest risk. This will result in efficient and effective use of both public and private resources, and avoid the diversion of scarce resources to low-priority tasks.

7.4 Utilize the results of existing projects in the field

Electric utilities in collaboration with DOE and NERC have completed many projects in the area of cybersecurity risk framework. JEA recommends that results of such projects be assessed and results be incorporated in the current assignment. These include the DOE sponsored study of cybersecurity risk for electric sector and the resultant ES-C2M2 (Capability Maturity Model).JEA has attached a copy and references in the appendix section of this submittal.

7.5 Consideration of Induced Risk on Critical Infrastructure

A study of many incidents that have impacted the critical infrastructure concluded that the risk was introduced from trusted systems outside the protected security zones (enclaves) that did not maintain appropriate cybersecurity standards or were not required to maintain compliance with any cyber security controls. Often these trusted systems leave these weaknesses because they do not have to comply with minimal competent cybersecurity controls. It is essential for such trusted systems that need connections and services from the critical infrastructure, to comply with minimal security standards, such as vulnerability mitigation, malware protections and appropriate access control.

8.0 Appendix – Referenced Resources

1. NERC CIP Standards
2. Electric Sector –Cybersecurity Capability Maturity Model
3. FRCC-NERC Compliance Monitoring & Enforcement Program