Bonneville Power Administration has a unique role and position, in that it participates in the Bulk Electric System subject to the provisions of the Energy Power Act of 2005 and the NERC Critical Information Protection (CIP) standards, and is a federal agency subject to regulations, directives and statutes such as the Federal Information Security Management Act of 2002 (FISMA). The CIP standards are compliance-based, whereas the standards and guidelines developed for FISMA by NIST are designed as a risk-based framework. Our experiences in these somewhat divergent but possibly complimentary programs are unique but not singular, as there are a handful of other federal electric utilities as well.

Our response to the RFI is not a direct response to each question as a federal agency. Rather, the intention is to provide the benefit of our experiences in the consideration of the Framework, and answer from the perspective of a member of the electricity sector.

1. RISK-BASED STANDARDS

Any new standards should take a risk-based approach. A risk-based approach enables utilities to implement the security measures that are most appropriate to mitigating the specific risks they face, in determining the best course of action for protecting their unique systems. Prescriptive and inflexible rule-based standards cannot keep pace with developments in the business application of technology, development of new technologies, and the ever-changing nature of threats.

What is most important is that the risks are understood by senior management and addressed. A culture of compliance often has unintended consequences, including not addressing risks for which the standards did not account.

As well, there are financial and operational burdens on an already strained workforce, possibly detracting utilities from protecting high-risk assets. It should be recognized that every utility's system is different and that a standard approach does not work. Developing new standards that allow for flexibility in addressing the risks to our specific systems will allow us to better protect against cyber threats.

2. RISK-BASED AUDITS

NERC-CIP audits have proved to be expensive, time consuming and don't necessarily make utility systems safer. Any new framework requiring an audit should focus the process to (1) identify and assess a utility's existing infrastructure/cyber assets used to support the Bulk Electric System (BES); (2)

implement appropriate security controls on each segment of our cyber system consistent with the criticality of those systems, based upon risk, which includes the threat information the federal government can provide and the impact that any threat might create; (3) assurance that the controls are functioning as intended, based on real-time monitoring and cyber security testing, and (4) a maturity model, such as the ES-C2M2, should be utilized to provide a context and basic model for performance-based measurements.

3. INCENTIVES FOR PARTICIPATION

The Framework should not create new auditing and compliance mechanisms for electric utilities separate and apart from those already required under NERC CIP. Utilities are already subject to rigorous NERC auditing and compliance and should not be subjected to a similar and additional process for newly developed standards separate from NERC. A wholly separate set of compliance requirements and oversight can end up becoming duplicative and needlessly costly to implement. Even when standards are similar, if the compliance processes are not, the end result is additional resources dedicated or allocated in a less than optimal way. One way to do this is for the Framework to allow for third party verification of compliance with any new risk-based standards, to be deemed as complying with existing mandatory standards. This administrative change would provide incentive for electric utilities and allow them to focus on protecting systems.

4. VENDORS /SUPPLY CHAIN STANDARDS

Vendors are a critical partner of utilities in meeting and exceeding existing or new cyber security standards. The Framework should help ensure that vendors build and improve cyber security capabilities of their products/appliances/solutions to allow security configurations to meet formal critical infrastructure security standards (e.g., NERC CIP) or security framework (e.g. NIST 800-53). There are many initiatives in the area of supply chain risk management whose ongoing work can be leveraged in developing this area of the Framework.

5. INCENTIVES FOR UPGRADE

Once improved cyber security capabilities are available they will need to be implemented to be of value. To expedite the replacement of devices containing these improvements, potential government incentives, subsidies or assistance in life cycle refreshing of legacy Bulk Electric System (BES) equipment should be available. Currently these legacy devices are not intended to be replaced sooner than a 15-25

year life and, consequently, even if vendors began introducing improved cyber security configurations today, entities may wait to actually implement those more secure/sophisticated devices, due to cost.

6. INFORMATION SHARING

Improvement in the area of information sharing between utilities and the government has been included in most comprehensive proposed or draft cyber legislation. This is an important step in promoting more secure systems, and must ensure timely and actionable sharing of information to be successful. Incentives and protections are likely necessary to promote participation. The federal government often has access to national security information that includes cyber security elements such as indicators or signatures that could be effective in reducing risks. There are methods by which such data can be used, without unauthorized disclosure of national security information. The Framework should include programs to allow the private sector to make use of this data using these or similar methods. Funding these programs and addressing the legal and regulatory protections that might be necessary are understandably outside the scope of the Framework and likely would require legislation. Addressing how such programs might work and funding or legal relief in legislation can be part of the Framework discussion or the Framework itself.

7. UTILIZE A MATURITY MODEL

Numerous cyber security frameworks exist. The U.S. DOE's Office of Electricity Delivery and Energy Reliability, with assistance from Carnegie Mellon University and participation from across the private sector, recently released the Electricity Subsector Cyber security Capability Management Maturity Model (ES-C2M2). Frameworks and maturity models allow organizations to identify their strengths and weaknesses and compare themselves against industry best practices. Use of tools like the ES-C2M2 allows organizations to improve management of risks and to improve operations. The Framework authors should consider utilizing a consistent and/or baseline security framework for performance based measurement. The ES-C2M2 can provide part of the Framework in terms of performance-based measurement.

Questions regarding this response can be directed to either of the following individuals:

- *Larry Buttress, Acting EVP of Internal Business Services* *ldbuttress@bpa.gov* *503-230-3690*
- *Gary Dodd, Chief Information Security Officer* *gadodd@bpa.gov* *503-230-4474*