UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure Protection Reliability Standards	**))**	**Docket No. RM15-14-000**

WRITTEN COMMENTS OF JOHN GALLOWAY, Ph.D. DIRECTOR OF CYBER SECURITY, ISO NEW ENGLAND INC.

Good morning, my name is John Galloway and I am the Director of Cybersecurity at ISO New England Inc. ("ISO-NE"). I want to thank the Commission for setting up this conference to discuss issues related to supply chain risk management and for providing me with an opportunity to speak.

In sum, ISO-NE supports the Commission's proposal to direct NERC to develop requirements relating to supply chain risk management. We believe that the risks to the reliability of the Bulk Electric System that result from compromised third-party software are real, significant and largely unaddressed by existing reliability standards. A new reliability standard that requires vendors to attest to their use of best practices is the best and simplest way to reduce these risks. While many public utilities are already assessing these risks and asking vendors to address them, these one-off efforts are far less likely to be effective than an industry-wide reliability standard. In my comments, I will address the four issues raised by the Commission.

1. Identify challenges faced in managing supply chain risk.

- o Number of possible risks multiplied by supply chain members (simple enumeration is a challenge)
- o Absence of current security testing and quality assurance practice in some supplier cases, for example, some software suppliers. While these notions may be new to a few companies that may be in the midst of trying to adopt such practices, in the case of a large, well-established operating system vendor like Microsoft these practices have been standard for years.

- Changes required to buy/build risk tradeoffs as part of regular project practices. Hand in hand with contracts – if you add supply chain risk – such changes to culture can take a while.
- Effective evaluation of enumerated risks to support prioritization and business decision making such as vendor selection and rating practices.
- A number of vendors may choose not to negotiate regarding contract terms for their security posture, especially large vendors. Attempts to contract for the protections we want may be difficult – having a reliability standard would increase the likelihood of success if all entities in the industry need the same protections.

2. Describe how the current CIP Standards provide supply chain risk management controls.

Version 5 of CIP-003, CIP-004, and CIP-005 address logical and physical controls for on-site vendors. In addition, version 5 of CIP-007 requires system security management controls for software supporting reliability functions. However, these existing reliability standards are far less comprehensive than we need. That said, they are precedents for NERC standards that require registered entities to manage their relationships with their vendors.

3. Describe how the current CIP Standards incentivize or inhibit the introduction of more secure technology.

- Incentive: existence of a reliability standard for cyber security promotes discussion of cyber security requirements for products and practices relevant to reliability functions; this simplifies and supports negotiation of contract terms for qualities of software being purchased as well as support of such systems.
- Inhibition: assumptions currently present in standard requirements regarding network and physical siting and access restrictions may make adoption of some technical measures when implementing reliability functions more difficult. Examples of recent advances in this type of technology are virtual networks/storage/systems and application clustering which support a very dynamic provision of services in multiple physical and network

locations. Significant improvements in resilience and availability may be possible with these more recent advances in technology, but the strict requirements for containment of services in single, particular Electronic Security Perimeters (ESPs) and Physical Security Perimeters (PSPs) may prove to be a challenge to implementing these services in a compliant manner given their dynamic nature.

4. Identify possible other approaches that the Commission can take to mitigate supply chain risks.

- The Commission could work with industry, the Department of Energy and NIST on an update to the Cyber Security Framework to include or further specify consideration of issues of supply chain risk management in that standard, but that framework is voluntary in nature and might not provide as much support for a contract negotiation as a mandatory reliability standard approved by the Commission.
- The Commission could direct NERC and industry to augment or enhance controls currently associated with CIP-007 relevant to supply chain risk management. This might involve extending CIP-007 regarding system security management controls, but this could increase administrative burden for handling of that particular reliability standard which has tended to be scoped in terms of systems already present at a given entity, as opposed to those being developed along the supply chain. This would be an indirect and perhaps not as well understood approach to the issue as compared to a reliability standard directly addressing management of supply chain risks.