UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

Statement of Thomas F. O'Brien

Vice President & Chief Information Officer

PJM Interconnection, L.L.C.

January 28, 2016

PJM Interconnection is pleased to provide these initial comments in response to the Commission's inquiry on the "Cyber Security Supply Chain Best Practices." My comments will address some of the unique challenges, current PJM actions, and a set of recommendations to further advance the supply chain cybersecurity issues.

I serve as the Vice President and Chief Information Officer for PJM. In this role, I oversee all aspects of PJM's information technology and enterprise information security. My role has been to ensure we are implementing technology to meet our responsibilities as an RTO in a secure and reliable manner.

I appreciate the Commission's focus on the importance of supply chain cybersecurity issues. Supply chain risk is a genuine threat that needs to be carefully considered and managed. The complexity and breadth of supply chain cybersecurity risk includes end-to-end management of the supply and distribution of hardware, firmware, system software, application software and services.

Effectively identifying and managing the cybersecurity risks within the supply chain is important. There are clear and documented examples across several supply chains and distribution channels of embedded attacks in hardware, system software, application software, and services. A risk-based approach will drive the greatest value by ensuring that we address the highest risks first.

Managing the supply chain from a cybersecurity perspective does create some unique challenges:

- **The supply chain is highly distributed and does not fall under any single regulatory jurisdiction, which potentially could subject hardware, software, and service vendors to diverse standards from multiple critical infrastructures and regulatory agencies: The supply chain does not lend itself to creating the necessary collaboration and accountability to ensure issues are managed by those best able to manage the risk;**

- **An ineffective regulatory program can create a false sense of security and divert resources from focusing on activities which are most within the customer's control; and**

- **Ineffective management of the supply chain for addressing cybersecurity issues could lead to increased utility costs without a corresponding significant benefit to the end user. Thus, it is critically important that we address supply chain cybersecurity risks in an efficient and cost-effective manner**

PJM is addressing the cybersecurity supply chain issues that the Commission has identified within the context of our overall security program. Our program has advanced significantly and has demonstrated tangible benefits in terms of advancing the cybersecurity of our systems through the PJM procurement process. Nevertheless, PJM recognizes the need for further enhancements as we manage the threats. Our collaboration with software, hardware, and services vendors has shown that

as one moves up the supply chain, cybersecurity supply chain practices are inconsistent and therefore must continue to evolve and improve.

By way of example, some of PJM's current activities that are focused on enhancing cybersecurity of our systems through our procurement process and other internal processes include:

- **Our participation in DHS classified briefings to better understand the cybersecurity threats including supply chain threats;**
- **Modifications to our vendor review process as part of our procurement processes to ensure that risk and cybersecurity best practices are carefully considered prior to contract approval;**
- **Analysis of cyber and physical security controls for major vendors of high risk systems to ensure that their internal security practices are sufficient to reduce unintentional defects as well as intentional infiltration of malware and backdoors;**
- **Development of common security requirements that will be part of our request for proposal process and technology implementations;**
- **PJM buying only from authorized resellers, avoiding used products to reduce the risk of counterfeit and tainted products;**
- **PJM requiring contractors and vendors to undergo PJM's background screening process irrespective of the criticality of that access;**
- **Engaging third parties for advanced security penetration testing on an annual basis and when major systems are released into production environments;**
- **Advanced 24x7 security event monitoring tools and controls to detect potentially malicious network activity that would result from tainted products;**
- **File system monitoring for high-risk systems to ensure that changes on file systems correspond to authorized changes;**
- **Establishment of a software management governance team to ensure that all software is authorized prior to installation and has gone through a security review;**
- **Participation in the Cyber Risk Information Sharing Program (CRISP), which provides detection of potentially malicious traffic that may result from nation state infiltration of supply chains.**

In light of the complexity, the existing disparate industry standards, the immaturity of supply chain cybersecurity practices among vendors, and the absence of well-established practices in supply chain cybersecurity, PJM proposes that, at this time, a directive to NERC to develop a standard in this area may not be the best use of time and resources to address this issue. Standard drafting is

something of a "cottage industry" with its own set of challenges focused on choice of specific words, action required and issues surrounding enforcement and penalties. Getting embroiled in these issues prematurely may take away from the kind of development of "best practices" guidance and cross-industry communication that is needed at this stage of the process. Accordingly, we would urge the Commission to consider other vehicles which could range from use of NERC's process for the development of Guidance Papers (a process which has been used by the Critical Infrastructure Protection Committee (CIPC) which is tasked to develop, periodically review, and revise security guidelines) to more organized Commission-sponsored communications both within the electric industry as well as across industries.[1] A similar effort for communication among regulators of different sectors especially impacted by cybersecurity, such as the financial and communication sectors in addition to the utility sector, would also help to advance supply chain cybersecurity capabilities and ensure the sharing of best practices.

As a result, our recommended path forward is to encourage cross sector coordination and collaboration with the providers in the technology industry as opposed to diverting focus to the drafting of a technical standard at this point in time. On the other hand, we do believe there is a key FERC and NERC role at this point in time. Presently, there are a host of standards and publications that need to be better coordinated and harmonized. These include:

- **NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations.**

- **ISO 20243 - Open Trusted Technology Provider Standard (O-TTPS) - A standard of the Open Group Vendors that provides a set of guidelines, recommendations and requirements that help assure against maliciously tainted and counterfeit products.**

- **Department of Energy's Cybersecurity Procurement Language for Energy Delivery Systems - This publication is a guidance document that provides baseline cybersecurity procurement language for use by asset owners, operators, integrators, and suppliers during the procurement process.**

- **NIST Cyber Security Framework - Provides guidance to help the energy sector establish or align existing cybersecurity risk management programs to meet the objectives of the Cybersecurity Framework released by the National Institutes of Standards and Technology (NIST) in February 2014.**

- **ISO 27000 Standards – Information Security Management Family of Standards.**

[1] The development of guidance documents in lieu of standards is specifically contemplated in the charters of certain NERC Committees including the CIPC. The full set of CIPC guidelines are available at: http://www.nerc.com/comm/CIPC/Pages/Security-Guidelines.aspx.

We would suggest that FERC direct NERC to develop a guidance document (using the existing CIPC guidance document process outlined above) as well as gather and synthesize key data on best practices in cybersecurity procurement as well as work with NIST and other agencies to rationalize the above standards and publications into a guidance document that works for the electric industry in light of its role as a buyer rather than manufacturer of these products. This should include collaboration with IT vendors and service providers to understand the current state and to develop a roadmap for improving vendor cybersecurity supply chain practices. The scope of this effort should include specific recommendations associated with best practices in implementation of the above standards in the context of procurement of software and hardware. For example, the guidance could include:

- **concepts on the ability to validate the authenticity of software and patches that are being downloaded;**
- **review of best practices associated with the procurement of hardware through specialized supply chains;**
- **best practices in application vulnerability management; and**
- **other specific recommendations based on the risk analysis.**

Nevertheless, although PJM feels this guidance process focused on detailing best practices as outlined above is a more appropriate first step at this point, should the Commission decide that it desires to move forward with a directive to NERC to develop a binding standard at this point, we believe that the focus and assignment should be on strengthening *the current CIP standards.* Under this scenario, the existing standards would be reviewed in light of best practices that have been identified to address the supply chain risk in the areas that registered entities control with respect to prevention, detection, and resilience.

Finally, we note the passage of recent legislation that authorizes increased communication and collaboration between the industry and the relevant federal agencies. We believe the passage of this long-overdue legislation provides the legal authority for FERC, working with DHS and NIST, to ensure greater reporting on cyber threats to the E-ISAC and improved two-way communications. These efforts should be focused on :

- **Providing transparency to cybersecurity risks embedded in commonly-used critical software applications and hardware; and**
- **Engaging with other critical infrastructures and government agencies (including other federal and state regulators) to ensure unity of approach.**

In short, we see this entire exercise, including this NOPR, as part of a continued evolution of best practices and collaboration across critical infrastructures and technology service providers. At the same time, we recognize that protection across all critical infrastructure sectors is beyond FERC jurisdiction. As a result, it will be imperative to continue the broader engagement with the Department of Homeland Security, NIST, other critical infrastructure sectors, technology providers, and other government agencies to enhance our management of the supply chain against cybersecurity threats.

PJM stands ready to work with the Commission, stakeholders, NERC, and others in that process.