UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Technical Conference on Critical Infrastructure Protection Supply Chain Risk Management — **Docket No. RM15-14**

Prepared Statement of Jonathan Appelbaum,
Director, NERC, The United Illuminating Company

Good afternoon members of the Commission staff. I am Jonathan Appelbaum, Director, NERC at The United Illuminating Company (UI). Thank you for the opportunity to participate in today's technical conference.

UI, a subsidiary of AVANGRID, Inc[1], is a New Haven-based regional electric distribution company engaged in the purchase, transmission, distribution and sale of electricity and related services to approximately 325,000 residential, commercial and industrial customers in the Greater New Haven and Bridgeport areas. We are subject to the mandatory Reliability Standards developed and enforced by the North American Electric Reliability Corporation.

UI supports the Trade Association comments submitted by the Edison Electric Institute, the American Public Power Association, the National Rural Electric Cooperative Association, Electricity Consumers Resource Council, Transmission Access Policy Study Group, and the Large Public Power Council in response the Commission's Notice of Proposed Rule Making issued under this docket last year. I appreciate the Commission holding the conference to continue

[1] AVANGRID, Inc. (AGR) is a diversified energy and utility company with $30 billion in assets and operations in 25 states. The company operates regulated utilities, electricity generation, and natural gas storage through three primary lines of business. Iberdrola USA Networks includes eight electric and natural gas utilities, serving 3.1 million customers in New York and New England. Iberdrola Renewables operates 6.3 gigawatts of electricity capacity, primarily through wind power, in states across the U.S. Iberdrola Energy Holdings operates 120 Bcf of owned or contracted natural gas storage and hub service facilities in the South and West.

this discussion.

UI acknowledges that there are challenges in managing supply chain risk, however we do not believe that a Reliability Standard or modifications to an existing Standard is needed to address supply risks for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. Although the Critical Infrastructure Protection Reliability Standards (CIP) do not specifically mention "supply chain," it is important to emphasize for the Commission that version 5 of these standards adequately addresses this risk and creates a strong incentive for Responsible Entities to work with their suppliers and vendors to further minimize this risk.

A Reliability Standard or modifications to an existing Standard is not appropriate given that a utility has very limited ability to influence risk beyond its organizational environment. For example, the NIST SP 800-161 definition of supply chain is "the integrated set of components (hardware, software, and processes) within the organizational boundaries that composes the environment in which a system is developed or manufactured, tested, deployed, maintained and retired/decommissioned."[2] Notice this definition scopes activities to those within the organization. The lifecycle of industrial control systems, which includes research, development, design, manufacturing, acquisition, delivery, integration, operations, retirement, and disposal, is not entirely within the organizational boundary of electric power utilities that own and operate the bulk electric system. The utility's environment or boundary in this supply chain is limited to acquisition through disposal.

Requiring utilities to manage risk in the research, development, design, and manufacturing

[2] NIST 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015), p. 5, *available at*: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

stages would transfer risk created and owned by suppliers to the Responsible Entity. These stages are in the supplier environment, the companies that manufacture industrial control systems and not within the utility environment. Also, a utility's influence in acquisition, delivery, and even disposal may be limited as third party suppliers also play a role in these stages.

Utilities can influence the acquisition and delivery stages through contract negotiations with their suppliers; however, this influence is limited. For example, let's assume a mandatory requirement for physical security monitoring of a supplier's security perimeter. A utility would contact the original equipment manufacturer and distributors and explain this requirement and inform the supplier of the need for physical security. The contract or purchase order is renegotiated to add additional terms. The utility would require audit evidence of the supplier's physical security monitoring. The supplier issues an annual letter stating their compliance to the contract, and the utility would perform a periodic verification inspection of the facility. If the supplier's monitoring system fails then the utility files a self-report of noncompliance and possibly receives an enforcement action for the supplier's process and management. For a supplier this is adding a great deal of cost and administrative cost to service one subclass of its customers. For the utility this is creating compliance risk, transferring a supplier's management risk to the utility, and not significantly improving the security posture of the utility. Therefore any requirement should be tied to the utility environment and organizational boundary, the utility's ability to control the risk, and the auditor's ability to verify the requirement is met in an audit. This is difficult in the acquisition and delivery stages and any improvement to reliability is likely minimal, especially when you look at the existing requirements of CIP version 5.

In order to actually improve reliability a mandatory requirement must be achievable. If a mandatory requirement is aspirational, that is the required processes are not established and may

not be developed, then the utility is administratively burdened to document these exceptions with no improvement to reliability. We have experienced this burden under the CIP version 3 framework.

CIP version 5, which introduces many new cybersecurity requirements and will bring many new systems under scope of these requirements, already provides very strong supply chain controls. For example, CIP-010 for cyber asset change management requires Responsible Entities to conduct extensive testing and vulnerability assessments prior to connecting BES Cyber Systems to their operating environment, and CIP-011 requires sanitizing or destroying media containing BES Cyber Security Information. These and the other requirements contained within CIP version 5 not only improve the reliability of the bulk electric system, but they create a strong incentive for utilities to incorporate cybersecurity requirements into their procurement process.

It is unclear to me how regulating utility procurement processes would improve reliability beyond the improvements already addressed by the CIP version 5 requirements. Instead, I see only challenges to such regulation. For example, new requirements could result in the abandonment of existing spare equipment in the utility's and supply chain's inventory. Additionally, onerous requirements may reduce the number of suppliers for a cyber asset. The NIST SP800-161 recognizes this and states:

> When organizations or system integrators require greater levels of transparency from suppliers, they must consider the possible cost implications of such requirements. Suppliers may select to not participate in procurements to avoid increased costs or perceived risks to their intellectual property, limiting an organization's supply or technology choices. The risk to suppliers is the potential for

multiple, different sets of requirements that they may have to individually comply with, which may not be scalable.[3]

In conclusion, instead of creating new mandatory requirements, I strongly recommend that the Commission allow time for implementation and enforcement of CIP version 5. Time and experience from these activities is needed to determine if there are any true reliability gaps that require new requirements. Thank you, I look forward to questions and further discussion.

[3] *Id*. at section 3.3.2.