

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

**Version 5 Critical Infrastructure Protection )  
Reliability Standards )**

**Docket No. RM13-5-000**

**Technical Conference Comments of Richard J. Dewey  
On Behalf of the New York Independent System Operator**

**I. INTRODUCTION**

My name is Richard Dewey. I am Senior Vice President and Chief Information Officer of the New York Independent System Operator. I joined the NYISO in 2000. The NYISO is responsible for operating the New York’s high-voltage transmission network, administering and monitoring the wholesale electricity markets, and planning for the state’s energy future. The Information Technology Group I oversee is responsible for delivering products and services to evolve the wholesale electricity markets; development, support, and maintenance of all NYISO software and systems; strategy development, technical design, and maintenance of the NYISO’s computing infrastructure; and maintaining the NYISO’s physical facilities and enterprise security. I have a Master of Science in Computer Engineering from Syracuse University and a Bachelor of Science in Electrical and Computer Engineering from Clarkson University in Potsdam, New York.

**II. COMMENTS**

**Background: CIP Version 5 and Networks Protection**

I would like to thank the Commission and FERC staff for the opportunity to participate in this Technical Conference to discuss the Critical Infrastructure Protection topics identified by the Commission in Order 791 and, more specifically, to participate in the panel on, and provide these

Comments, regarding the adequacy of the approved CIP version 5 standards for protecting data being transmitted over Bulk Power System communication networks.

The NYISO, working with its stakeholders, peer ISOs/RTOs, and the broader electricity industry, strives to be a leader in addressing cybersecurity issues related to the protection of critical infrastructure. To that end, the NYISO regularly participates in standards development processes, works with industry groups, and engages in regional, national, and international planning initiatives addressing future technology and security integration. The NYISO is currently supporting the Standard Drafting Team addressing NERC Project 2014-02 CIP version 5 revisions, formed to address the points raised by the Commission in Order 791.

Keeping the lights on is always the primary focus for the NYISO. Cybersecurity is critical to that effort. The NYISO recognizes the importance of robust CIP standards, and notes that standards such as CIP-005 have protected electric grid operations from cyber attacks such as the Shamoon by using computer network segmentation to restrict access to the critical infrastructure. But would-be attackers quickly adapt, and so must industry by continuously evolving our security posture in response to rapidly changing risks, threats, and technological advances. In this way, cybersecurity standards must enable rather than hinder continuous improvement.

The NYISO supports the trend in cybersecurity rulemaking toward standards that are not needlessly prescriptive, but rather—where appropriate—give entities the latitude to identify and assess enterprise-specific risks and develop appropriate controls to mitigate them. The NIST framework is an excellent example of such an approach. Given the substantial volume of sensitive data the NYISO must constantly exchange with its market participants, neighboring control areas and other interested parties, securing our communication networks is particularly

essential. With respect to the NERC CIP Version 5 Revisions now underway at NERC, the NYISO recognizes that concepts such as the use of strong encryption and Network Access Controls are elements that any user or operator of a communications network must strongly consider. At the same time, we recognize the inherent difficulty of drafting cybersecurity standards that reflect the varying needs of industry members with different network topologies. To that end, the NYISO urges NERC and the Commission to employ a risk-based methodology for any new or revised CIP standards related to communication networks in order to encourage and leverage well-tailored and cost-effective controls like those that will be described further in these comments. Communications network protection will necessarily involve a combination of architectures, technologies, and embedded solutions such as monitoring. Entities should be empowered by any new or revised standards to find the combination of these controls that are appropriate to the levels and types of risk they identify.

### **NYISO and Industry Initiatives for Communications Network Security**

The telecommunications industry—a distinct critical infrastructure in its own right—is a driving force for enabling innovation by electric utilities. With the advent of new telemetering sources like Phasor Measurement Units (PMUs), coupled with the need to monitor the dynamic characteristics that other technologies like battery storage, increased renewable energy, microgrids, and distributed generation are adding to the grid, the need for real-time or near real-time data has never been greater. Advancements in communications networking provide means to collect and disseminate data with greater ease and at ever increasing rates; as the electric industry becomes increasingly reliant on such data exchange, securing communication networks grows ever more critical. I would like to make the Commission aware of two initiatives

reflecting how the electric industry is proactively addressing the need for secure communication networks.

First, the NYISO is supporting an effort by our industry and its trade groups to implement a Department of Energy-supported effort to identify appropriate Cyber Security Procurement Language for Control Systems. Despite our industry's heavy reliance on networking, telecommunications remains a complementary yet separate form of infrastructure – this means that, at least for the foreseeable future, we are heavily reliant on external service providers to assist us in developing and securing our communication networks. By collaborating to identify and document best practices for cybersecurity technology, including for networks protection, industry is developing a common language to communicate to and obtain from its vendors the security architecture needed to accomplish its core purposes.

Second, in the spring of 2013, the NYISO and other Reliability Coordinators in the Eastern Interconnection cataloged a number of operations data transfer mechanisms that occur through a variety of mediums. We identified an opportunity to provide additional capabilities—particularly as PMU data is incorporated into situational awareness—and a shared desire to investigate mechanisms to obtain consistency and efficiencies in securely managing these data exchanges. That effort culminated in formation of the Eastern Interconnect Data Sharing Network, Inc. (EIDSN), a non-profit corporation formed in January 2014. The EIDSN is positioned to build and coordinate the reliable and secure exchange of critical infrastructure information amongst its members. Its design team is currently identifying the security architectures necessary to safely share critical operational information. The EIDSN will translate those requirements into a Request for Information and Request for Proposal for bidders to propose solutions to provide these essential services for the organization and the industry. It will

rely on the Cyber Security Procurement Language for Control Systems discussed above and our collective experience with Smart Grid projects to help ensure security is embedded into the life cycle of EIDSN services and products.

Initiatives like the Cyber Security Procurement Language for Control Systems and EIDSN demonstrate the commitment of the NYISO and our industry to promoting and enhancing secure networking capabilities that reflect evolving needs and demands. Just as importantly, these are real world examples of industry's success in identifying risks and relying on its expertise to develop means to mitigate that risk. Any additional CIP version 5 standard language should reflect this approach.

#### **NYISO and Industry Efforts in Support of Cybersecurity Information Sharing**

As cybersecurity matures, tools to share sector-specific security information quickly and securely grow increasingly important. One such tool is the Reliability Coordinator Information Sharing portal, which enables the exchange of incident and threat-based information along with reliability data. Electric industry reliability coordinators and balancing authorities are uniquely situated at the crossroads of this information exchange, possessing strong system visibility and operational knowledge to interpret this data, maintain grid reliability, and restore operations after an event. Secure communication networks are vital to leveraging those capabilities.

More broadly, industry continues to work with public and private organizations to improve sharing of cyber and physical security threat information and assessments, to support its core business practices, and in response to Executive Order 13636 and Presidential Policy Directive 21. The Electric Sector Information Sharing Analysis Center (ES-ISAC), working with government partners, is aiding this effort with its Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) coordination activities. The Department of Energy-

supported “Cyber Risk Information Sharing Program” (CRISP) and “Cyber Fed Model” (CFM) offer promise for developing enhanced and cost-effective tools to increase information-sharing gain situational awareness. NERC’s GridEx II preparedness exercise in November 2013 also demonstrated industry improvements in sharing security related information. NYISO fully participated in NERC’s GridEx II exercise with many other organizations, agencies and entities; communications and information sharing, along with regional coordination, led to a successful exercise.

### **III. CONCLUSION**

New technologies introduced into the Electric Grid provide both promise and challenge. The ability to collect and disseminate new, more detailed metering will drive more advanced applications and greater capabilities to address the challenge of incorporating renewable sources of energy into the grid. Enhanced capabilities for management and monitoring of battery storage, flywheel, microgrid, and distributed generation technologies will allow these new grid elements to meet the full potential of delivering resilient and reliable energy for consumers. Better identification and sharing of situational-awareness and threat-based information between and among industry and government will enhance critical infrastructure reliability. Communications networking is critical to addressing all these needs. Appropriate, risk-driven security measures must and will be applied as we grow and evolve the communications networks used in our industry. The NYISO looks forward to addressing this challenge with industry and government partners.

Dated: April 28, 2014