UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Policy Issues Related to the Reliability of the Bulk-Power System	**Docket No. AD17-8-000**

PRE-TECHNICAL CONFERENCE STATEMENT OF COMMISSIONER ROBERT R SCOTT OF THE NEW HAMPSHIRE PUBLIC UTILITIES COMMISSION

June 13, 2017

I. INTRODUCTION

Pursuant to the Federal Energy Regulatory Commission's ("FERC or the Commission") May 19, 2017 Supplemental Notice of Technical Conference, this pre-technical conference statement is submitted consistent with my authority as Commissioner of the New Hampshire Public Utilities.

As noted in the May 19 Supplemental Notice, panelists are asked to discuss policy issues related to the reliability of the Bulk-Power System. In particular, I have been asked to present on the topic of grid security and what actions should be considered to improve cybersecurity. I thank the Commission for convening this technical conference and for allowing me to share with you my thoughts on these important topics.

II. STATEMENT

Cybersecurity is understood to be an increasingly important element ensuring reliable operation of the electric grid. Recent events such as the 2015 cyberattack on electricity distribution control centers and 2016 attack on electricity transmission facilities in the Ukraine and the inaccurate press reports regarding the Vermont municipal utility Burlington Electric Department have highlighted the potential vulnerability of the grid here in the United States. From a risk perspective, the FERC jurisdictional bulk-power system and the State regulated electric

distribution companies are interdependent and a risk mitigation strategy for one cannot succeed without addressing the other. Further, at least as it applies to New England, the cybersecurity functions for both the transmission and distribution components of our major electric utility companies are centrally managed. The same staff and systems that protect the Bulk-Power System also protect the distribution systems. Measures to protect the Bulk-Power System are, where appropriate, used to protect distribution systems. Similarly, given the nature of these systems, threats to the distribution system can endanger the larger grid.

Partnerships to help improve the overall cybersecurity posture

The New England states have endeavored to build relationships with our utility, state and federal partners. The New England states in concert with our regional organization, the New England Conference of Public Utilities Commissioners, are working together on this important issue. In New Hampshire, through our administrative rule process, we put in place a requirement for our regulated electric distribution companies to submit an annual physical and cyber security plan to the commission. Given that the electric distribution utilities have affiliates in other New England states, and the utility cybersecurity is generally centrally managed for all affiliates, New Hampshire invites regulators and staff from neighboring states to attend these meetings with the utilities.

As part of this effort of fostering information sharing and continuous improvement, we invited FERC's Office of Energy Infrastructure Security (OEIS) to attend one such set of meetings so that they could review our utility's plans and make suggestions for improvements. In addition to conducting the reviews and participating in the joint meetings, OEIS also offered to conduct architectural reviews of utility network systems, further identifying vulnerabilities.

One of the best ways to ensure a proper response in the event of an incident, both for the states and the utilities, is to prepare in advance and develop working relationships. In preparing to be able to respond to a cyber incident, the New England states engaged with FERC's OEIS in developing a cyber incident response checklist. This is an important step in being able to conduct exercises to further build relationships and learn in advance of an actual emergency. Last week, many of our important partners, including New England utilities, regulators, ISO New England Inc., United States Department of Homeland Security Office of Intelligence and Analysis, and the National Guard worked together in the New England National Guard's annual Cyber Yankee exercise, ensuring a better understanding of how the National Guard can assist in protecting and if need be restoring the electric grid from a cyber attack.

Security clearances

As part of our capacity building efforts in New England, OEIS was able to work with the intelligence community to facilitate one day classified read-ins for Commissioners. This helped ensure that state regulators understood the risks posed by cybersecurity threats. Next month, OEIS is again facilitating a similar briefing, but this time including utility executives and some of our other federal partners including the Office of the Director of National Intelligence, the Department of Homeland Security (DHS) and the Department of Energy.

At the outset of the New England effort, this region was unique and indeed in a special circumstance as we had three commissioners from three states, all with top secret or higher security clearances that had been carried over from previous work. This allowed meetings with the intelligence community and initiatives in other regions that provided us with a sense of the importance of our utilities being able to communicate at a classified level.

Working with DHS in particular, we are ensuring that appropriate utility and state regulatory personnel receive the security clearances needed to allow issues regarding cyber threat indicators to be identified and resolved. Allowing proper information sharing at this level is an important component in protecting our electric grid.

Workforce development at the state commission level

State commissions are generally not staffed to be able to evaluate or assess cybersecurity issues. As the Commission knows, our focus has been traditionally more aligned towards economic regulation. Cybersecurity represents a new skill set for the states. Developing expertise on this front will take some time. The National Association of Regulatory Utility Commissioners has done some good ground work on this topic, publishing a primer and offering instructional classes for state regulatory staff. However this continues to present a challenge, particularly to small state regulatory commissions.

Our partners in the Maine Public Utilities Commission are hiring someone who is retiring from his work with United States Cyber Command early next month. Given his background, Maine intends to make this employee available as a regional asset, assisting with our common cybersecurity initiatives. While there is much more to be done in developing expertise at the states, this is the type of regional approach that states should emulate.

Finally, I wish to point out the importance of FERC's Office of Energy Infrastructure Security. OEIS offers ready assistance to the states on security matters, provides needed expertise and advice, and provides a vital bridge between state regulators and other federal and industry partners. They are a vital component of our efforts in New England and are appreciated by the states.

Thank you for providing this venue to hear the views of states regarding this impactful issue.

Respectfully Submitted,

Robert R. Scott
Commissioner, New Hampshire Public Utilities Commission
21 S. Fruit Street
Concord, NH 03301-2429
(603) 271-2290