UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Technical Conference	)	Docket No. AD18-11-000

Statement of William J. Fehrman
President and CEO, Berkshire Hathaway Energy
on Behalf of The Edison Electric Institute

July 31, 2018 Reliability Technical Conference
Panel I: The Changing ERO Enterprise, Standards, and Reliability

Good Morning, I am Bill Fehrman, the President and CEO of Berkshire Hathaway Energy. On behalf of the Edison Electric Institute ("EEI") and EEI's members, thank you for the opportunity to participate in today's technical conference and for providing a forum to discuss the reliability of the bulk-power system ("BPS"), the Reliability Standards, and the ERO Enterprise that develops and enforces these standards.

Berkshire Hathaway Energy is a diversified global holding company that owns subsidiaries principally engaged in energy businesses in the United States, Canada, Great Britain, and the Philippines. The Berkshire Hathaway Energy businesses include MidAmerican Energy Company, PacifiCorp, NV Energy, Inc., BHE Pipeline Group, BHE Renewables, BHE U.S. Transmission, AltaLink, L.P., Northern Powergrid Holdings Company, as well as HomeServices of America, Incorporated.

EEI is the association that represents all U.S. investor-owned electric companies. EEI members provide electricity for about 220 million Americans, and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. EEI's members are committed to providing affordable and reliable electricity to customers now and in the future.

EEI's diverse membership includes electric utilities that own and operate the electric grid. As a result, reliability of the grid is not only essential to our customers and the Commission, but our employees and investors. Delivering electricity to customers is the primary mission of EEI's members, which requires maintaining an affordable, reliable, and resilient grid.

With respect to the specific reliability issues raised for discussion during the first panel, I will focus on:

(1) Addressing the evolving risks to reliability;

(2) Improving the efficiency and effectiveness of the Reliability Standards and the ERO Enterprise; and

(3) Managing change in the Western Interconnection.

1. Evolving Risk to Reliability.

The evolving risks to grid reliability, primarily security and the changing generation resource mix, warrant the most attention by NERC. Security requires vigilance and continuous improvement because of the dynamic and quickly evolving nature of threats. New technologies to help grid owners and operators defend their systems are also evolving. To meet these challenges, security defenses must be flexible to allow grid owners and operators to anticipate and adapt to the threats using the best tools available. The types of resources that are generating electricity are also changing. The increasing use of natural gas; the expansion of renewable, distributed, and asynchronous resources on the BPS; and advancing technologies each introduce new reliability challenges. For example, essential reliability services must be maintained and new technologies must be integrated into the planning, operations, and security of the BPS.

The Commission has been focused on cybersecurity for more than a decade through development and modification of the Critical Infrastructure Protection ("CIP") Reliability Standards and requirements, including a new supply chain cybersecurity risk management

standard. Implementing the supply chain requirements creates a unique challenge for industry because it will require significant, unprecedented coordination among procurement, legal, compliance, human resources, cybersecurity, and information technology stakeholders within companies as well as significant engagement and coordination with vendors to ensure that new requirements are thoroughly and effectively addressed.

In the January 2018 Notice of Proposed Rulemaking, the Commission proposed to shorten the implementation period for these new requirements from 18 to 12 months.[1] Although discrete actions to mitigate supply chain cybersecurity risks can be taken rapidly—such as mitigating a specific and pre-defined vendor risk—the comprehensive nature of the new CIP requirements will require significant coordination and analysis to thoroughly and effectively identify and address risk to the BPS. I encourage the Commission to allow for 18 months to ensure effective implementation of these requirements. Meanwhile, NERC is currently studying the nature and complexity of cybersecurity supply chain risks to develop recommendations for additional follow-up actions.[2] I encourage the Commission to allow NERC to finish this work before directing modifications to the new supply chain cybersecurity requirements. This work must be finished to provide industry and policy makers with a sound technical basis to guide efforts that effectively and efficiently manage reliability risk.

The CIP standards provide a strong regulatory foundation for protecting the BPS, but additional tools are necessary to address the dynamic and evolving nature of threats to cybersecurity. The industry is investing significant resources in the Electricity Information Sharing and Analysis Center ("E-ISAC"), operated by NERC, to provide timely sharing of

[1] *Notice of Proposed Rulemaking*, *Supply Chain Risk Management Reliability Standards*, 162 FERC ¶ 61,044 (2018).
[2] NERC, *Supply Chain Risk Mitigation Program*, available at: https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.

security threat information. I have personally dedicated significant time advising the E-ISAC and look forward to realizing the improvements in the analytical and information sharing capabilities that will help industry rapidly detect and mitigate threats. NERC and the industry must continue to focus on this important work, including ensuring that any resulting improvements are an effective and efficient use of industry resources in responding to security threats.

As detailed in the State of Reliability Report,[3] NERC is focused on security as well as the challenges to reliability arising from the changing generation resource mix. NERC's reliability assessments, which identify potential risks to reliability and potential methods to mitigate this risk, are important to industry and policy makers because they provide the technical basis needed to make the informed decisions that are critical to maintaining cost-effective and reliable service to customers.

2. Efficiency and Effectiveness of the Reliability Standards and the ERO Enterprise.

Due to the evolving reliability risks and limited industry resources, ensuring the Reliability Standards are effective and efficient in addressing reliability and security in planning, operations, and security is paramount. The Standards Efficiency Review initiative that NERC is undertaking, with the support of industry, reviews the existing Reliability Standards to identify opportunities to improve efficiency, which is important to helping industry prioritize resources. EEI supports NERC's risk-based review of the Reliability Standards to identify potential efficiencies. The risk-based review will ensure that reliability and security is maintained, while tailoring—through modification or retirement—the existing standards to be more efficient.

[3] NERC, *State of Reliability 2018* (Jun. 2018), available at: https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_2018_SOR_06202018_Final.pdf

EEI also supports NERC's efforts to improve the efficiency and effectiveness of the ERO Enterprise, including activities such as the effectiveness framework for stakeholder committee engagement. Additionally, continued enhancement of NERC's risk-based compliance and enforcement program to ensure compliance is appropriately tailored to focus on identifying, prioritizing, and addressing risk to the BPS will help to improve efficiencies and consistency throughout the ERO Enterprise and industry, as well as allow for the proper allocation of resources. NERC is also developing an enterprise-wide tool for its compliance monitoring and enforcement program ("CMEP"). This tool promises to make the CMEP program more effective and efficient by replacing the individual regional entity tools with one, common tool that will help to improve consistency across the ERO Enterprise in the execution of compliance monitoring and enforcement. However, putting all of this information in one spot will create new cybersecurity challenges as the information collected will include sensitive critical infrastructure information that identifies grid vulnerabilities. The aggregation of this information represents a "one stop shop" for threat actors. I encourage NERC and the Commission to prioritize information protection wherever such information is collected, stored, or transferred.

3. Changes in the Western Interconnection.

The transition from a single Reliability Coordinator ("RC") to multiple RCs and expansion of the organized wholesale markets in the Western Interconnection requires collaboration and coordination among a variety of entities. The utilities in the Western Interconnection recognize the importance of a strong RC and are working with NERC and WECC to ensure the reliability of the BPS. Balancing Authorities and Transmission Operators are currently evaluating the RC service providers in the Western Interconnection to determine the best option for reliability and their customers. The reliability considerations during this

transition includes the management of seams, communication protocols during planned and unplanned outages, and consistency of RC models across the interconnection. Additionally, ensuring that the RC is NERC certified and meets the requirements of an RC is important for reliability of the BPS. NERC and WECC are focused on ensuring that these issues are managed to prevent reliability impacts.

In conclusion, I appreciate the opportunity to participate in this technical conference as it provides a needed forum to discuss the important issues associated with reliability. The Commission, NERC, and the industry all have a shared commitment to reliability of the BPS. We support continuing work to enhance reliability and security through risk-based compliance monitoring and enforcement, the E-ISAC, and technical analysis that will help industry identify and mitigate challenges created by advancing technology and threats. We look forward to collaborating with the Commission, NERC, and stakeholders in considering solutions that support our collective efforts to ensure continued BPS reliability and security.

Document Content(s)