UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Technical Conference Docket No. AD17-8-000

PRE-TECHNICAL CONFERENCE STATEMENT OF BRANDON WALES, DIRECTOR DEPARTMENT OF HOMELAND SECURITY OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS

Executive Summary

Good afternoon Acting Chairwoman LaFleur, Commissioner Honorable, and assembled staff and thank you for the opportunity to address the Federal Energy Regulatory Commission today on behalf of the Department of Homeland Security's National Protection and Programs Directorate (NPPD). NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure from all hazards. NPPD works with partners at all levels of government, and from the private and non-profit sectors, to share information and build greater trust to make our cyber and physical infrastructure more secure. This includes a working relationship with a number of FERC staff offices, including the Office of Electric Reliability and the Office of Energy Infrastructure Security.

I oversee the Office of Cyber and Infrastructure Analysis within NPPD, whose mission is to support efforts to protect the Nation's critical infrastructure through an integrated analytic approach evaluating the potential consequences of disruption from physical or cyber threats and incidents. The analysis produced by my office supports decisions to strengthen infrastructure security and resilience, as well as response and recovery efforts during natural hazards and man-made incidents.

My testimony today will focus on two issues of interest in response to the panel questions in the conference agenda. The first issue covers the need for traditional electric utility planning activities to embrace cyber based contingencies and the second issue focuses on the efforts of the Department of the Homeland Security to increase and enhance information sharing and analysis activities with the electric sector.

1) **The importance of including cyber-based contingencies in system planning studies to ensure the continued reliable operation of the electric grid in response to all hazards.**

As electric utilities adapt (and potentially increase) their use of industrial control systems to automate and increase the efficiency of operations, the cyber related consequences of the adoption of new practices and procedures should be carefully studied and evaluated to understand the potential impact of their loss or disruption to reliable operation of the electric grid.[1] Cyber hazards do not have well characterized likelihood and consequences to critical infrastructure assets and systems and cyber events can simultaneously occur over large geographic areas without respect to traditional boundaries of electric system operations or control. These events may stress traditional emergency management and response procedures designed to contain and constrain system problems.[2]

To understand potential system impacts, a natural evolution may be for system planners to create a number of cyber contingency cases which could incorporate a variety of cyber issues that may affect system monitoring or communications disruptions and impact infrastructure

[1] Detailed models of industrial control systems and their use in supporting system operations are not easily accessible to system operators, system planners, and cybersecurity professionals. This can lead to a lack of understanding from system operators in understanding what events are normal system events versus cybersecurity events. This also impedes the development of simulations which accurately represent the reaction of the system to events.

[2] This could lead to electric utilities developing potentially inaccurate forced outage rates for equipment and systems in response to events and disrupt carefully constructed contingency response activities.

operations. The loss of communications and monitoring could occur directly at a wide-area integrator of this data, such as a reliability coordinator, or this event could occur simultaneously at a number of balancing authorities who provide data to a reliability coordinator to ensure wide-area situational awareness to events.[3] Cyber scenarios should have characteristics distinct from current hazards to challenge the utilities understanding of the degree of the impact possible from a cyber event.

A potential outcome would be for electric utilities to better understand how cyber security staff are deployed within their organization, and look to further embed cyber security expertise into traditional electric utility functional areas where appropriate, with the likely areas including long-term system planning and real-time system operations. This step is intended to not only enhance utilities response to contingencies of cyber events, but also for electric utilities to better understand the cyber and communication characteristics for existing contingencies which depend upon cyber connected components. The long-term outcome of this effort is a more robust consideration of contingencies from both a physical and cyber perspective, leading to greater system resilience from all hazards.

2) **Ensuring the sharing of potentially sensitive security information between the private sector and the federal government in near real-time to support decision-making by critical infrastructure owners and operators.**

The Department of Homeland Security works with partners at all levels of government, and from the private and non-profit sectors, to share information and build greater trust to make our cyber and physical infrastructure more secure. This includes sharing information through platforms such as the Critical Infrastructure Partnership Advisory Council (CIPAC), the Electric

[3] Inadequate regional-scale visibility over the bulk power system and the failure to identify and communicate that status to neighboring systems are two primary recommendations included within the final report of the U.S.-Canada Power System Outage Task Force for the August 2003 northeast blackout and the Federal Energy Regulatory Commission's evaluation of the 2011 Arizona-Southern California electric outage.

Subsector Coordinating Council (ESCC), and physical and cybersecurity operation centers of the Department including the National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC). Information and analysis released by the NICC and NCCIC may be subsequently shared to electric sector owners and operators through the Electricity Information Sharing and Analysis Center (E-ISAC).

The Department's cybersecurity authorities and functions derive from various statutes and associated presidential direction. These statutes and presidential directives authorize the Department to accomplish three missions in cybersecurity: (1) Information sharing and technical assistance activities involving federal entities, non-federal entities, including international partners; (2) Protection of federal information and information systems; and, (3) Coordination of the federal government's response to cyber incidents.

One of the DHS's most prominent initiatives to enhance information sharing between the Federal Government and private sector that I would like to highlight is called Automated Indicator Sharing (AIS).[4] AIS connects participating organizations to a DHS-managed system at the NCCIC that allows bi-directional sharing of cyber threat indicators, helping to build a common, shared knowledge of current cyber threats. AIS is a part of the Department's effort to create an ecosystem where as soon as a company or federal agency observes an attempted compromise, the indicator will be shared in real time with all of our partners, enabling them to protect themselves from that particular threat. This means adversaries can only use an attack once, which increases their costs and ultimately reduces the prevalence of cyber attacks. While

[4] AIS is available for free through the DHS NCCIC, a 24/7 cyber situational awareness, incident response, and management center which was designated as the central hub for the sharing of cyber threat indicators between the private sector and the Federal Government by the Cybersecurity Act of 2015. This legislation also grants liability protection and other protections to companies that share indicators through AIS. More information on AIS is available here: https://www.us-cert.gov/ais

AIS won't eliminate sophisticated cyber threats, it should allow participating organizations to concentrate on more complex events by mitigating less sophisticated attacks.

Another initiative to facilitate information sharing is the Cyber Information Sharing and Collaboration Program (CISCP) which enables the sharing of cybersecurity threat information in a secure fashion with entities across critical infrastructure sectors. CISCP provides for analytical collaboration between DHS and participating entities (which include non-profit industry groups presenting entire sectors of critical infrastructure) and when appropriate, allows participating entities to embed analysts on the NCCIC watch floor.

The final point I will raise on information sharing is that more analysis is needed to better understand requirements for both data collection and analysis of data by critical infrastructure owners and operators. While the electric sector is an exception in data collection and management, in that, the sector has well defined methods and procedures to identify and track system changes over time, this is not the case across all critical infrastructure sectors.

Future cyber events may not directly target electric power owners and operators, but may impact connected infrastructure systems which the bulk electric system depends to ensure reliable operations. As our information technology systems become further interconnected and interwoven, disruptions will no longer be limited to a single infrastructure asset or system; consequences can be far reaching. Long-term, this may necessitate the development of a common information model that can be applied across all critical infrastructures sectors to understand dependencies and interdependencies between infrastructure assets and systems.

Conclusion

The issues I have raised here today are complex and don't lend themselves to easy, "silver bullet" solutions. The Department of Homeland Security is committed to working with

FERC and other partners in the electric sector to begin working these and other challenges facing the systems that power our country. Thank you for your time and I am available to take your questions.