May 27, 2016

FEDERAL ENERGY REGULATORY COMMISSION

2016 State of Reliability	**)**	**Docket No. AD16-15-000**

RELIABILITY TECHNICAL CONFERENCE

WRITTEN STATEMENT BY L. DEVON STREIT
DEPUTY ASSISTANT SECRETARY FOR INFRASTRUCTURE SECURITY AND ENERGY RESTORATION
OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY
U.S. DEPARTMENT OF ENERGY

JUNE 1, 2016

Thank you for the opportunity to express the views of the Department of Energy (DOE) on a range of important issues related to energy grid security. The office of Infrastructure Security and Energy Restoration (ISER), under the Office of Electricity Delivery and Energy Reliability (OE), is responsible for the Department's efforts to lead Emergency Support Function #12 – Energy, and to coordinate the Federal response supporting state and local efforts during incidents affecting energy infrastructure caused by physical or cyber threats. During steady state activities, as a division of the Sector Specific Agency for Energy, ISER works with other Federal agencies, with industry partners, and with regulators to ensure that the Nation's energy supply is prepared and resilient. In this written statement, I will address topics raised in questions provided by the Federal Energy Regulatory Commission (FERC) in advance of the panel on Grid Security at the Reliability Technical Conference on June 1st, 2016.

I. Cybersecurity Authorities and Information Sharing

a. The Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the Fixing America's Surface Transportation (FAST) Act both addressed cybersecurity. Discuss how government, NERC and industry can use these new authorities to address cybersecurity risks and enhance information sharing.

The Fixing America's Surface Transportation (FAST) Act (P.L. 114-84) has granted DOE the authority, in the context of a "Grid Security Emergency" declared by the President, to issue emergency orders to protect or restore the reliability of critical electric infrastructure or defense-related critical electric infrastructure during the Emergency. As directed under the FAST Act, DOE is developing proposed rules of procedure for expediting orders in the context of an Emergency, and will continue its partnership with the energy sector to maximize the effectiveness of this authority.

The FAST Act has also codified the delegation to DOE made in Presidential Policy Directive 21 – DOE is the Sector-Specific Agency for cybersecurity for the energy sector. The Department continues to evolve its cybersecurity role as the technology landscape changes. We currently offer several preparedness programs that help address cybersecurity risks and facilitate information sharing.

One of these programs is the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2), developed jointly by DOE and industry partners. C2M2 helps private sector owners and operators better assess their own cybersecurity posture. It provides a self-evaluation tool that helps organizations evaluate, prioritize, and improve their own cyber capabilities. Since C2M2 was initiated in June 2012, more than 750 organizations have requested and received the program's toolkit, including more than 400 electricity subsector organizations. Participation in

the program continues to grow, and represents a concrete step that all energy sector companies can take to improve their own cyber security.

Another initiative is the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership co-funded by DOE and industry partners that develops situational awareness tools that enable the energy sector to better protect critical infrastructure and key resources through the exchange of detailed cybersecurity information. CRISP uses advanced sensors and threat-analysis techniques to keep the energy sector informed of high-level cyber risks. Current participants in CRISP provide power to more than fifty percent of continental U.S. electricity customers.

II. Technology Risks and Lessons Learned

b. What can we learn from recent attacks, and what should we do in response? Are there ways to reduce risk by "simplifying" or even non-digitizing the technology used at certain critical points or locations? Are there reasonable ways to further reduce the risk of lengthy outages from hostile actions, and can new standards or changes to standards help?

Lessons learned from previous incidents have confirmed that the power grid is, to a great extent, a robust eco-system that can survive an unusual attack, such as the one that occurred on April 16, 2013 against the Metcalf substation near San Jose, California, without experiencing widespread and extended power outages. Emerging threats posed by new technology capabilities nonetheless make energy infrastructure security a constantly evolving challenge. Regardless of the resilience of the Nation's power grid, a sustained effort is required to protect critical assets.

While a variety of methods must be employed to address the consistent challenge posed by cyber threats, a technology regression that favors "simplifying" or "non-digitizing" grid

technology may increase risk in the area of operations. Digital technologies, including relays utilizing synchrophasors, allow many enhancements to the reliability of grid operations that would be lost by failing to employ technological advancements that improve the future grid and its capabilities. Instead of looking backwards and considering how to maintain previous benchmarks, a forward-looking approach is needed, one that favors the development of security features that are integrated into the design of components on the front end. Security must be tied into the advances that make the grid smarter and more resilient.

One measure that can reduce the risk of lengthy outages is to increase the availability of key equipment spares so that more transformers and other pieces of equipment are readily available to quickly replace damaged items. Additionally, manufacturing processes for critical technologies can emphasize the expeditious production of spare components. Several industry programs, including Grid Assurance, STEP, Wattstock, and Spare Connect, are working to improve access to equipment during the industry's moment of need. Such efforts will improve restoration times and improve customer satisfaction by ensuring that power is restored more efficiently as a result of faster access to replacement equipment.

The Strategic Transformer Reserve, contemplated within the FAST Act, could become a key tool for minimizing the impact of power grid disruptions. A reserve may increase the availability of spare transformers and emergency mobile substations that are staged at predesignated locations for timely delivery in the aftermath of an energy grid disruption. The FAST Act directs DOE, in consultation with other stakeholders, to develop a plan to establish the Reserve, and to this end we have asked Oak Ridge National Laboratory to lead a technical analysis of the feasibility of establishing the Reserve.

DOE, its Pacific Northwest National Laboratory, the North American Electric Reliability Corporation (NERC), and a number of industry experts recently worked together to develop the Design Basis Threat (DBT) guide to help the electricity sector address the physical security of substations and to help utilities determine threats to their assets. This guide enables companies to make risk-based decisions with respect to their security investments.

III. Reliability Standards

c. *How effectively does the current standards process address emerging or rapidly evolving reliability issues? Can Reliability Standards be structured to change quickly for newly-identified security risks or new scientific or engineering analyses (e.g., of geomagnetic disturbances)? If so, how?*

This is a topic that is not ultimately part of OE's portfolio, and is best addressed by NERC and FERC as the organizations responsible for Reliability Standards. The standards are an important mechanism for ensuring an interconnected and reliably operated grid, and provide a clear set of regulations for utilities to comply with. However, they can also impose significant costs to technology providers or to users that they may not be able to pass on to their customers. An examination of possible approaches to including new or changed technology in the rate base of utilities would be useful. Including industry in discussions is essential for building effective and realistic regulations to ensure reliability.

IV. Transportation of Transformers

d. Is progress being made on standardization and transportation of transformers to facilitate timely replacements after an emergency? Are there actions the Commission should consider to encourage progress?

The Strategic Transformer Reserve, as addressed in the FAST Act, is envisioned as a program that would improve the handling and deployment of spare transformers and emergency mobile substations in the aftermath of major impacts to the electric grid. In general, the use of strategic storage locations for reserve equipment could ease logistics challenges and allow transformers to be efficiently transported to areas of need. Both government and industry organizations are pursuing this concept.

Edison Electric Institute (EEI) has formed a Transformer Transportation Working Group to address this issue, and has been working with the Class I Railroads to plan for possible events that would require the movement of transformers. Industry efforts to reduce unit weight, are critical innovations, and using multiple ports could help with transportation logistics following an emergency. Reducing the number of transformer classes may occur over the long term as transformers are phased out, but many are not interchangeable even within classes.

V. EMP Research

e. What is the status of research on whether or how electromagnetic pulses might affect the grid? What additional research would help address any uncertainties?

We know that an electromagnetic pulse (EMP), if strong enough, can disrupt or damage electrical equipment, including critical computers and communications equipment that allow for smart operation of the energy grid. DOE and the Department of Homeland Security (DHS) are funding a new project with Los Alamos National Laboratory that will identify the EMP attack scenarios that are of most concern to the energy sector.

While other agencies, such as DHS, have more of a direct role in addressing the impact of potential EMP events as national security threats, DOE and the Electric Power Research Institute

jointly have drafted a preliminary EMP Resilience Strategy that will lead to further action plans and steps to mitigate the effects of EMP events on energy infrastructure.

In an effort that will enable robust responses to a range of possible scenarios, including, but by no means exclusive to, EMP events, DOE and FEMA are working together on a Power Outage Incident Annex that will help determine the optimal steps to take to quickly restore power when faced with a long-term power outage.

More scientific testing is needed to determine the vulnerability of all equipment and components associated with power plants and substations, including different transformers, to different levels of EMP effects.

VI. Reliability Standards Violations

f. The CIP and PRC standards continue to be among the most-often violated Reliability Standards. What efforts are being made, or should be made, to improve compliance with these particular standards?

This topic is principally addressed by NERC and FERC, which are most qualified to address Reliability Standards violations and efforts to improve compliance.

Concluding Statement

Protecting the energy grid is critical to our Nation's future. As potential hazards become more challenging and more complex, we must maintain a consistent and collaborative public-private partnership to prepare for and mitigate the effects of physical and cyber challenges. I appreciate the opportunity to address a number of thought-provoking questions about the resilience and security of our Nation's energy infrastructure.