



## **FERC/DOE Security Investments for Energy Infrastructure Technical Conference**

**Docket No. AD19-12-000**

**Thursday, March 28, 2019**

**10:00 a.m. – 4:00 p.m.**

The Commission has a well-developed set of mandatory and enforceable reliability standards that set baseline protections for both cyber and physical security of the bulk electric system. Moreover, the Commission has well established policies that allow for the opportunity to recover prudently incurred costs to comply with those mandatory reliability standards. This technical conference is aimed at better understanding (1) the need for security investments that go beyond those measures already required by mandatory reliability standards, including in infrastructure not subject to those standards (e.g., natural gas pipelines); (2) how the costs of such investments are or could be recovered; and (3) whether additional incentives for making such investments are needed, and if so, how those incentives should be designed.

**10:00 a.m. Opening Remarks and Introductions**

**10:30 a.m. Panel I: Cyber and Physical Security, Best Practices, and Industry and Government Engagement**

**Objectives:** This panel will discuss types of cyber and physical security threats to energy infrastructure, particularly electric transmission, generation, and natural gas pipelines. In addition, the panel will explore best practices for cyber and physical security mitigation beyond those measures already required by mandatory reliability standards and industry and government engagement needed to address these matters. Panelists will be asked to address the following:

***Threats to Energy Infrastructure:***

1. What cyber and physical security threats are most concerning for the energy industry? What critical factors should industry consider when evaluating the risk these threats present and prioritizing risk-mitigating security initiatives to address these threats?
2. Does industry have adequate resources to evaluate sophisticated threats such as whether adversaries have established access to their networks, whether insider threats exist, or whether supply chain equipment or subcomponents are compromised?

3. How are interdependencies among energy infrastructure sectors considered in risk management analyses?
4. What are some of the challenges (e.g. staffing or technology), that industry faces, in order to keep current with the threats?
5. What other current or emerging threats should be addressed? For example, what are some of the types of physical and cyber security threats that Unmanned Aircraft Systems (i.e., drones) can present? What experience has industry had with commercially-available products used to address these issues?

***Mitigation: Strategies and Best Practices:***

6. What are some of the best practices that industry uses to ensure effective action against cyber and physical security threats? Are adequate tools available for industry to assess where to apply best practices (e.g., risk management analyses) for cyber and physical security threats? Do these analyses differ between cyber and physical security threats?
7. How does industry validate the effectiveness of, and maintain its mitigation techniques/measures (e.g., red teaming, manufacturers recommendations) for, both physical and cyber protection? What are the processes to confirm the results are addressed? Are these lessons shared with others in the industry?
8. What resources are available to assist industry in evaluating risk to energy infrastructure and implementing mitigation measures, especially for small to medium size owners and operators?
9. What training opportunities are available to owners and operators to understand the various risks to their energy infrastructure and the measures taken to mitigate against physical and cyber threats? What training is necessary and not available?
10. How does industry mitigate key vulnerabilities to address disruptions from a cyber or physical attack or an extreme natural event (e.g. geomagnetic disturbance)? How should spare equipment, sharing programs, contractor and mutual assistance programs, and other processes be considered in addressing disruptions? What role should the federal government play in helping industry prevent and respond to disruptions? What preparations should be made by industry to assure adequate response and recovery efforts?

**Panelists:**

- William R. Evanina; Director, Office of the Director of National Intelligence, National Counterintelligence and Security Center
- Robert Kolasky; Director, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, National Risk Management Center
- Charles P. Kosak; Deputy Assistant Secretary, Department of Defense, Defense Continuity and Mission Assurance
- Sonya T. Proctor; Assistant Administrator of Surface Operations Department of Homeland Security, Transportation Security Administration, Security Operations

- Nicholas K. Akins; President and CEO, American Electric Power
- Mark A. Gabriel; Administrator and CEO, Western Area Power Administration
- James B. Robb; President and CEO, North American Electric Reliability Corporation
- Thomas J. Galloway; President and CEO, North American Transmission Forum
- Donald F. Santa; President and CEO, Interstate Natural Gas Association of America

**12:30 p.m. Lunch Break**

**1:45 p.m. Panel II: Incentives and Cost Recovery for Security Investments**

**Objectives:** This panel will explore how federal and state authorities can provide incentives and cost recovery for security investments in energy infrastructure, particularly electric transmission, generation, and natural gas pipeline infrastructure. Panelists will be asked to address the following:

***Cost Recovery:***

1. What role do states currently play in requiring and/or facilitating energy infrastructure security investments? Do states require industry to have plans and programs to prevent and recover from cyber and physical attacks? Is industry subject to requirements to assess risk and prioritize action based on state priorities?
2. Are current cost recovery policies of the federal and state governments affecting the ability of owners and operators of energy infrastructure to invest in cyber and physical security for this energy infrastructure? Do federal and state policies complement or conflict with each other? Are these policies helping or hindering security investments?
3. Do cost recovery policies at the state and federal level facilitate the adoption of best practices for threat mitigation at energy infrastructures? Do they allow for cost recovery for investment to address mitigation of new and emerging threats (e.g., intentional electromagnetic interference and electromagnetic pulse)?
4. Is FERC's September 14, 2001 Statement of Policy on Extraordinary Expenditures Necessary to Safeguard National Energy Supplies<sup>1</sup> still helpful to facilitate investment that supports physical and cyber security of energy infrastructure, or are any revisions to the Policy Statement needed to facilitate such investment?
5. For competitive generators that do not recover their costs through retail rates, are there mechanisms under which they may recover costs for physical or cybersecurity investments other than through their market-based rates?
6. If federal standards, guidelines, or authorities indicate that an energy facility is high-risk or critical (i.e., designation as Defense Critical Electric Infrastructure under Section 215A of the Federal Power Act), how would such designations be considered as a company prioritizes security investments? How would such a designation be considered by state regulators when reviewing cost recovery filings for measures taken above and beyond

---

<sup>1</sup> *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies*, 96 FERC ¶ 61,299 (2001) (Policy Statement).

compliance with mandatory reliability standards?

7. What factors should the states be aware of when reviewing cost recovery filings for cyber and physical security investments? Can these factors be included on an industry-wide or multi-state level?
8. Certain events could require significant unbudgeted resources to respond effectively. How should these costs be considered by federal and state authorities for cost recovery?

***Financial Incentives:***

9. What type of incentives would be most effective to facilitate investment in cyber and physical security? How could costs for these incentives be recovered?
10. How could the Commission use its authority under Section 219 of the Federal Power Act to establish incentives for improved cyber and physical security? Are there other ratemaking or accounting changes that would help incent investments in cyber and physical security?
11. Are there any grants or other cost recovery mechanisms available for industry to assist with security investments at their facilities?
12. What changes could federal and state authorities make to current policies to better incent the adoption of best practices for cyber and physical security at energy infrastructure facilities?
13. How should state and federal authorities prioritize incentives for various security investments? How should such incentives balance the need for improved security with the rate impact on consumers?

**Panelists:**

- Christopher M. Crane; President and CEO, Exelon Corporation
- Nicholas A. Brown; President and CEO, Southwest Power Pool, Inc.
- Jay Scott Emler; Commissioner, Kansas Corporation Commission
- Kevin G. Wailes; CEO, Lincoln Electric System and Co-Chair, Electricity Subsector Coordinating Council
- Paul Kjellander; Commissioner, Idaho Public Utilities Commission
- Alan S. Armstrong; President and CEO, Williams
- Upendra J. Chivukula; Commissioner, New Jersey Board of Public Utilities

**3:45 p.m. Closing Remarks**

**4:00 p.m. Adjourn**