

word-processing formats. Documents created electronically using word-processing software should be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

41. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426.

42. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

#### IV. Document Availability

43. In addition to publishing the full text of this document in the **Federal Register**, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the internet through the Commission's Home Page (<http://www.ferc.gov>) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. eastern time) at 888 First Street NE, Room 2A, Washington, DC 20426.

44. From the Commission's Home Page on the internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

45. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or email at [ferconlinesupport@ferc.gov](mailto:ferconlinesupport@ferc.gov), or the Public Reference Room at (202) 502-8371, TTY (202) 502-8659. Email the Public Reference Room at [public.referenceroom@ferc.gov](mailto:public.referenceroom@ferc.gov).

By direction of the Commission.

Issued: March 21, 2019.

**Nathaniel J. Davis, Sr.,**  
Deputy Secretary.

[FR Doc. 2019-05893 Filed 3-27-19; 8:45 am]

**BILLING CODE 6717-01-P**

## DEPARTMENT OF ENERGY

### Federal Energy Regulatory Commission

[Docket No. AD19-12-000]

#### Security Investments for Energy Infrastructure Technical Conference; Supplemental Notice of Technical Conference

Take notice that the Federal Energy Regulatory Commission (Commission) and the United States Department of Energy (DOE) will co-host a Security Investments for Energy Infrastructure Technical Conference (conference) on Thursday, March 28, 2019, from 10:00 a.m. to 4:00 p.m. This Commissioner- and DOE senior official-led conference will be held in the Commission Meeting Room at the Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426. The purpose of the conference is to discuss current cyber and physical security practices used to protect energy infrastructure and will explore how federal and state authorities can provide incentives and cost recovery for security investments in energy infrastructure, particularly the electric and natural gas sectors. Attached is the final agenda for this event with the confirmed list of panelists.

The conference will be open and free to the public; however, interested attendees are encouraged to preregister online at: <https://www.ferc.gov/whats-new/registration/03-28-19-form.asp>. In-person attendees should allow ample time to pass through building security procedures before the 10:00 a.m. start time of the conference.

The Commission intends to solicit post-technical conference comments and will issue a public notice with further directions following the conclusion of the conference.

Information regarding the conference will be posted on the Calendar of Events on the Commission's website, <http://www.ferc.gov>, prior to the event. The conference will also be webcast and transcribed. Anyone with internet access who desires to listen to this event can do so by navigating to the Calendar of Events at <http://www.ferc.gov> and locating this event in the Calendar. The event will contain a link to the webcast. The Capitol Connection provides technical support for webcasts and offers the option of listening to the meeting via phone-bridge for a fee. If you have any questions, visit <http://www.CapitolConnection.org> or call (703) 993-3100. Transcripts of the technical conference will be available for a fee

from Ace-Federal Reporters, Inc. at (202) 347-3700.

Commission conferences are accessible under section 508 of the Rehabilitation Act of 1973. For accessibility accommodations, please send an email to [accessibility@ferc.gov](mailto:accessibility@ferc.gov) or call toll free 1 (866) 208-3372 (voice) or (202) 502-8659 (TTY), or send a fax to (202) 208-2106 with the required accommodations.

For more information about this technical conference, please contact Carolyn Templeton by phone at (202) 502-8785 or by email at [carolyn.templeton@ferc.gov](mailto:carolyn.templeton@ferc.gov). For information related to logistics, please contact Sarah McKinley at (202) 502-8368 or by email at [sarah.mckinley@ferc.gov](mailto:sarah.mckinley@ferc.gov).

Dated: March 21, 2019.

**Nathaniel J. Davis, Sr.,**  
Deputy Secretary.

#### 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 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

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

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

[FR Doc. 2019-05894 Filed 3-27-19; 8:45 am]

BILLING CODE 6717-01-P

## DEPARTMENT OF ENERGY

### Federal Energy Regulatory Commission

[Docket No. EL19-56-000]

#### Hoosier Energy Rural Electric Cooperative, Inc.; Notice of Filing

Take notice that on March 20, 2019, Hoosier Energy Rural Electric Cooperative, Inc., filed a proposed revenue requirement for reactive supply and voltage control for the Lawrence Generating Station, Merom Generating Station, and Worthington Generating Station, under Midcontinent Independent System Operator Inc. Tariff Schedule 2.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211, 385.214). Protests will be considered by the Commission in determining the appropriate action to be taken, but will not serve to make protestants parties to the proceeding. Any person wishing to become a party must file a notice of intervention or motion to intervene, as appropriate. Such notices, motions, or protests must be filed on or before the comment date. On or before the comment date, it is not necessary to serve motions to intervene or protests on persons other than the Applicant.

The Commission encourages electronic submission of protests and interventions in lieu of paper using the "eFiling" link at <http://www.ferc.gov>. Persons unable to file electronically should submit an original and 5 copies of the protest or intervention to the Federal Energy Regulatory Commission, 888 First Street NE, Washington, DC 20426.

This filing is accessible on-line at <http://www.ferc.gov>, using the "eLibrary" link and is available for review in the Commission's Public Reference Room in Washington, DC. There is an "eSubscription" link on the website that enables subscribers to receive email notification when a document is added to a subscribed docket(s). For assistance with any FERC Online service, please email [FERCOnlineSupport@ferc.gov](mailto:FERCOnlineSupport@ferc.gov), or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

*Comment Date:* 5:00 p.m. Eastern Time on April 10, 2019.

**Nathaniel J. Davis, Sr.,**

*Deputy Secretary.*

[FR Doc. 2019-05899 Filed 3-27-19; 8:45 am]

BILLING CODE 6717-01-P

## ENVIRONMENTAL PROTECTION AGENCY

[EPA-HQ-OW-2004-0013; FRL-9990-95-OEI]

### Information Collection Request Submitted to OMB for Review and Approval; Comment Request; EPA Strategic Plan Information on Source Water Protection (Renewal)

**AGENCY:** Environmental Protection Agency (EPA).

**ACTION:** Notice.

**SUMMARY:** The Environmental Protection Agency (EPA) has submitted an information collection request (ICR),

EPA Strategic Plan Information on Source Water Protection (EPA ICR Number 1816.07, OMB Control Number 2040-0197) to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act. This is a proposed renewal of the ICR, which is currently approved through March 31, 2019. Public comments were previously requested via the **Federal Register** on November 9, 2018 during a 60-day comment period. This notice allows for an additional 30 days for public comments. A fuller description of the ICR is given below, including its estimated burden and cost to the public. An agency may not conduct or sponsor and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.

**DATES:** Additional comments may be submitted on or before April 29, 2019.

**ADDRESSES:** Submit your comments, referencing Docket ID Number EPA-HQ-OW-2004-0013, to (1) EPA online using [www.regulations.gov](http://www.regulations.gov) (our preferred method), by email to the OW Docket at [OW-Docket@epa.gov](mailto:OW-Docket@epa.gov), or by mail to: the OW Docket, EPA Docket Center, Environmental Protection Agency, Mail Code 28221T, 1200 Pennsylvania Ave. NW, Washington, DC 20460, and (2) OMB via email to [oir\\_submission@omb.eop.gov](mailto:oir_submission@omb.eop.gov). Address comments to OMB Desk Officer for EPA.

EPA's policy is that all comments received will be included in the public docket without change including any personal information provided, unless the comment includes profanity, threats, information claimed to be Confidential Business Information (CBI) or other information whose disclosure is restricted by statute.

**FOR FURTHER INFORMATION CONTACT:**

Sherri Comerford, Drinking Water Protection Division—Prevention Branch, Office of Ground Water and Drinking Water, (MC 4606M), Environmental Protection Agency, 1200 Pennsylvania Ave. NW, Washington, DC 20460; telephone number: 202-564-4639; fax number: 202-564-3756; email address: [Comerford.Sherri@epa.gov](mailto:Comerford.Sherri@epa.gov).

**SUPPLEMENTARY INFORMATION:**

Supporting documents, which explain in detail the information that the EPA will be collecting, are available in the public docket for this ICR. The docket can be viewed online at [www.regulations.gov](http://www.regulations.gov) or in person at the EPA Docket Center, WJC West, Room 3334, 1301 Constitution Ave. NW, Washington, DC. The telephone number for the Docket Center is 202-566-1744. For additional information about EPA's