(d) Terminating agreements in whole or in part to the greatest extent authorized by law if an award no longer effectuates the program goals or agency priorities (2 CFR 200.340).

VI. Award Administration Information

1. *Award Notices:* If your application is successful, we notify your U.S. Representative and U.S. Senators and send you a Grant Award Notification (GAN); or we may send you an email containing a link to access an electronic version of your GAN. We also may notify you informally.

If your application is not evaluated or not selected for funding, we notify you.

2. *Administrative and National Policy Requirements:* We identify administrative and national policy requirements in the application package and reference these and other requirements in the *Applicable Regulations* section of this notice.

We reference the regulations outlining the terms and conditions of an award in the *Applicable Regulations* section of this notice and include these and other specific conditions in the GAN. The GAN also incorporates your approved application as part of your binding commitments under the grant.

3. *Open Licensing Requirements:* Unless an exception applies, if you are awarded a grant under this competition, you will be required to openly license to the public grant deliverables created in whole, or in part, with Department grant funds. When the deliverable consists of modifications to pre-existing works, the license extends only to those modifications that can be separately identified and only to the extent that open licensing is permitted under the terms of any licenses or other legal restrictions on the use of pre-existing works. Additionally, a grantee or subgrantee that is awarded competitive grant funds must have a plan to disseminate these public grant deliverables. This dissemination plan can be developed and submitted after your application has been reviewed and selected for funding. For additional information on the open licensing requirements please refer to 2 CFR 3474.20.

4. *Reporting:* (a) If you apply for a grant under this competition, you must ensure that you have in place the necessary processes and systems to comply with the reporting requirements in 2 CFR part 170 should you receive funding under the competition. This does not apply if you have an exception under 2 CFR 170.110(b).

(b) At the end of your project period, you must submit a final performance report, including financial information, as directed by the Secretary. If you receive a multiyear award, you must submit an annual performance report that provides the most current performance and financial expenditure information as directed by the Secretary under 34 CFR 75.118. The Secretary may also require more frequent performance reports under 34 CFR 75.720(c). For specific requirements on reporting, please go to *www.ed.gov/fund/grant/apply/appforms/appforms.html.*

5. *Performance Measures:* For purposes of Department reporting under 34 CFR 75.110, the Department will use the following performance measures to evaluate the success of the RDI grant program:

(a) For Absolute Priorities 1 and 3, the following program-level performance measures:

(1) The annual number of doctoral students enrolled at the lead applicant university.

(2) The annual number of doctoral conferrals.

(3) The annual number of doctoral conferrals to underrepresented students.

(4) Annual faculty development expenditures.

(5) The annual research and development expenditures in:

(i) Science and engineering.

(ii) Non-science and engineering.

(b) For Absolute Priority 2, the following program-level performance measures:

(1) The annual research and development expenditures in:

(i) Science and engineering.

(ii) Non-science and engineering.

(2) Annual faculty development expenditures.

VII. Other Information

Accessible Format: On request to the program contact person listed under **FOR FURTHER INFORMATION CONTACT**, individuals with disabilities can obtain this document and a copy of the application package in an accessible format. The Department will provide the requestor with an accessible format that may include Rich Text Format (RTF) or text format (txt), a thumb drive, an MP3 file, braille, large print, audiotape, or compact disc, or other accessible format.

Electronic Access to This Document: The official version of this document is the document published in the **Federal Register**. You may access the official edition of the **Federal Register** and the Code of Federal Regulations at *www.govinfo.gov.* At this site you can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Portable Document Format (PDF). To use PDF you must have Adobe Acrobat Reader, which is available free at the site.

You may also access documents of the Department published in the **Federal Register** by using the article search feature at *www.federalregister.gov.* Specifically, through the advanced search feature at this site, you can limit your search to documents published by the Department.

Nasser H. Paydar,

Assistant Secretary for Postsecondary Education.

[FR Doc. 2023–16402 Filed 8–1–23; 8:45 am]

BILLING CODE 4000–01–P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. RD23–2–000]

North American Electric Reliability Corporation; Supplemental Notice of Joint Technical Conference

As announced in the Notice of Joint Technical Conference issued in this proceeding on May 30, 2023, the Federal Energy Regulatory Commission (Commission) and North American Electric Reliability Corporation (NERC) staff will convene a technical conference on August 10, 2023, from 9:00 a.m. to 4:30 p.m. Eastern Time.

The purpose of this conference is to discuss physical security of the Bulk-Power System, including the adequacy of existing physical security controls, challenges, and solutions. The conference will include two parts and four panel discussions. Part 1 will address the effectiveness of Reliability Standard CIP–014–3 (Physical Security) and include two panels on the applicability of CIP–014–3 and minimum levels of physical protection. Part 2 will address solutions beyond Reliability Standard CIP–014–3 and include two panels on physical security best practices and operational preparedness and planning a more resilient grid.

Attached to this Supplemental Notice is an agenda for the technical conference, which includes more detail for each panel. Only invited panelists and staff from the Commission and NERC will participate in the panel discussions. Interested parties may listen and observe, and written comments may be submitted after the conference in Docket No. RD23–2–000.

The conference will be held in-person at NERC's headquarters at 3353 Peachtree Road NE, Suite 600, North

Tower, Atlanta, GA 30326. Information on travelling to NERC's Atlanta office is available here. The conference will be open for the public to attend, and there is no fee for attendance. It will be transcribed and webcast. Those observing via webcast may register here. Those who would like to attend in-person must register here. Space is limited for in-person attendance and therefore registration is required. In-person attendees are encouraged to ensure they have a confirmed in-person registration prior to finalizing any travel plans. Information on this conference will also be posted on the Calendar of Events on the Commission's website, *www.ferc.gov,* prior to the event.

Commission conferences are accessible under section 508 of the Rehabilitation Act of 1973. For accessibility accommodations, please send an email to *accessibility@ferc.gov,* call toll-free (866) 208–3372 (voice) or (202) 208–8659 (TTY), or send a fax to (202) 208–2106 with the required accommodations. The conference will also be transcribed. Transcripts will be available for a fee from Ace Reporting, (202) 347–3700.

For more information about this technical conference, please contact Terrance Clingan at *Terrance.Clingan@ferc.gov* or (202) 502–8823. For information related to logistics, please contact Lonnie Ratliff at *Lonnie.Ratliff@nerc.net* or Sarah McKinley at *Sarah.McKinley@ferc.gov* or (202) 502–8004.

Dated: July 27, 2023.

Kimberly D. Bose,

Secretary.

Joint Physical Security Technical Conference

Agenda

Docket No. RD23–2–000

August 10, 2023

August 10, 2023 | *9:00–4:30 p.m. Eastern*

NERC Atlanta Office, 3353 Peachtree Road NE, Suite 600—North Tower, Atlanta, GA 30326

Welcome and Opening Remarks (9:00–9:12 a.m.)

NERC Antitrust Compliance Guidelines and Commission Staff Disclaimer (9:12–9:15 a.m.)

Agenda

Introduction and Background (9:15–9:30 a.m.)

Commission and NERC staff will provide background information relevant to discussion during the technical conference, including on Reliability Standard CIP–014–3, the current physical security landscape, recent Commission activities on physical security, and the NERC report filed with the Commission in April.

Part 1: Effectiveness of Reliability Standard CIP–014–3

Part 1 of the technical conference will focus on Reliability Standard CIP–014–3, as it is enforced today as well as any potential revisions to the standard resulting in subsequent versions.

Panel 1—Applicability (9:30–10:50 a.m.)

This panel will explore the facilities subject to Reliability Standard CIP–014–3. While the NERC report filed with the Commission did not recommend revising the applicability section of the Standard at this time, the report determined that this could change based on additional information. Panelists will discuss whether the applicability section of Reliability Standard CIP–014–3 identifies the appropriate facilities to mitigate physical security risks to better assure reliable operation of the Bulk-Power System. Panelists will also discuss whether additional type(s) of substation configurations should be studied to determine risks and the possible need for required protections.

This panel may include a discussion of the following topics and questions:

1. Is the applicability Section of CIP–014–3 properly determining transmission station/substations to be assessed for instability, uncontrolled separation or cascading within the Interconnection? Specifically, are the correct facilities being assessed and what topology or characteristics should the applicable facilities have to be subject to CIP–014? For example, are there criteria other than those in Section 4.1.1 of CIP–014–3, such as connected to two vs. three other station/substations and exceeding the aggregated weighted value of 3000, changing the weighting value of the table in the applicability section, or including lower transmission voltages?

2. Given the changing threat landscape, are there specific transmission station/substation configurations that should be included in the applicability section of CIP–014–3, including combinations of stations/substations to represent coordinated attacks on multiple facilities? What would they be and why?

3. What other assessments (*e.g.,* a TPL–001 planning assessment) may be used to identify an at-risk facility or group of facilities that should be considered for applicability under CIP–014–3? How stringent are those assessments? Describe any procedural differences between those other assessments and the CIP–014–3 R1 Risk Assessment. Should CIP–014–3 apply to entities other than those transmission owners to which 4.1.1 applies or transmission operators to which 4.1.2 applies?

4. Should potential load loss or generation loss be considered? If so, why, and how would potential impact be determined (*e.g.,* how would potential load loss be determined in advance of running an assessment?)?

5. Should facilities that perform physical security monitoring functions that are not currently subject to CIP–014–3 (*e.g.,* security operation centers) be covered by CIP–014–3 as well? If so, what criteria should be used?

Panelists:

- Mark Rice, Pacific Northwest National Lab
- Representative, Office of Cybersecurity, Energy Security, and Emergency Response (Department of Energy)
- Adam Gerstnecker, Mitsubishi Electric Power Products, Inc.
- Jamie Calderon, NERC
- Lawrence Fitzgerald, TRC Companies

Break (10:50–11:00 a.m.)

Panel 2—Minimum Level of Physical Protection (11:00 a.m.–12:30 p.m.)

This panel will discuss the reliability goal to be achieved and based on that goal, what, if any, mandatory minimum resiliency or security protections should be required against facility attacks, *e.g.,* site hardening, ballistic protection, etc. This panel will discuss the scope of reliability, resilience, and security measures that are inclusive of a robust, effective, and risk-informed approach to reducing physical security risks. The panel will also consider whether any minimum protections should be tiered and discuss the appropriate criteria for a tiered approach.

This panel may include a discussion of the following topics and questions:

1. What is our reliability goal? What are we protecting against to ensure grid reliability beyond what is required in the current standards?

a. What are the specific physical security threats (both current and emerging) to all stations/substations on the bulk electric system?

b. As threats are continually evolving, how can we identify those specific threats?

c. How do threats vary across all stations/substations on the bulk electric system? How would defenses against those threats vary?

To what extent should simultaneous attacks at multiple sites be considered?

2. Do we need mandatory minimum protections? If so, what should they be?

a. Should there be flexible criteria or a bright line?

b. Should minimum protections be tiered (*i.e.,* stations/substations receive varying levels of protection according to their importance to the grid)? How should importance be quantified for these protections?

c. Should minimum protections be based on preventing instability, uncontrolled separation, or cascading or preventing loss of service to customers (*e.g.,* as in Moore County, NC) ? If minimum protections were to be based on something other than the instability, uncontrolled separation, or cascading, what burden would that have on various registered entities? If the focus is on loss of service, is it necessary to have state and local jurisdictions involved to implement a minimum set of protections?

d. In what areas should any minimum protections be focused?

i. Detection?

ii. Assessment?

iii. Response?

3. To what extent would minimum protections help mitigate the likelihood and/or reliability impact of simultaneous, multi-site attacks?

Panelists:

- Travis Moran, NERC/SERC
- Mike Melvin, Edison Electric Institute
- Kathy Judge, Edison Electric Institute
- Jackie Flowers, Tacoma Public Utilities
- Representative, American Public Power Association

Lunch (12:30–1:00 p.m.)

Part 2: Solutions Beyond CIP–014–3

Part 2 of the technical conference will focus on solutions for physical security beyond the requirements in Reliability Standard CIP–014–3.

Panel 3—Best Practices and Operational Preparedness (1:00–2:30 p.m.)

This panel will discuss physical security best practices for prevention, protection, response, and recovery. The discussion will include asset management strategies to prepare, incident training preparedness and response, and research and development needs.

This panel may include a discussion of the following topics and questions:

1. What is the physical security threat landscape for each of your companies? What best practices have been implemented to mitigate the risks and vulnerabilities of physical attacks on energy infrastructure?

2. What asset management and preparedness best practices have your member companies implemented to prevent, protect against, respond to, and recover from physical attacks on their energy infrastructure?

3. What research and development efforts are underway or needed for understanding and mitigating physical security risks to critical energy electrical infrastructure?

4. What research and development efforts, including the development of tools, would you like to see the National Labs undertake to assist your companies in addressing physical threats to your critical electrical infrastructure?

5. What do you need or would like to see from the energy industry to improve your ability and accuracy in addressing physical security risks to critical energy electrical infrastructure?

6. What best practices are in place to accelerate electric utility situational awareness of an incident and to involve local jurisdiction responders?

7. What can the federal and state regulators do to assist the energy industry in improving their physical security posture?

8. What training improvements can NERC and the Regional Entities implement to system operators to aid in real-time identification and recovery procedures from physical attacks?

9. What changes could be made to improve information sharing between the federal government and industry?

Panelists:

- Gupta Vinit, ITC Holdings Corp.
- Randy Horton, Electric Power Research Institute
- Craig Lawton, Sandia National Lab
- Michael Ball, Berkshire Hathaway Energy
- Thomas Galloway, North American Transmission Forum
- Scott Aaronson, Edison Electric Institute

Break (2:30–2:40 p.m.)

Panel 4—Grid Planning To Respond to and Recover From Physical and Cyber Security Threats and Potential Obstacles (2:40–4:10 p.m.)

This panel will explore planning to respond to and recovery from physical and cyber security threats and potential obstacles to developing and implementing such plans. This discussion will focus on how best to integrate cyber and physical security with engineering, particularly in the planning phase. The panel will discuss whether critical stations could be reduced through best practices and how to determine whether to mitigate the risk of a critical station or protect it. Finally, the panel will consider the implications of the changing resource mix on vulnerability of the grid and its resilience to disruptions.

This panel may include a discussion of the following topics and questions:

1. How can cyber and physical security be integrated with engineering, particularly planning? What aspects of cyber and physical security need to be incorporated into the transmission planning process?

2. What modifications could be made to TPL–001 to bring in broader attack focus (*e.g.,* coordinated attack)? What sensitivities or examined contingencies might help identify vulnerabilities to grid attacks?

3. Currently, if a CIP–014–3 R1 assessment deems a transmission station/substation as ''critical'' that station/substation must be physically protected. Are there best practices for reconfiguring facilities so as to reduce the criticality of stations/substations?

4. When prioritizing resources, how should entities determine which ''critical'' stations/substations to remove from the list and which to protect? If the project is extensive and may have a long lead time to construct, to what degree does the station/substation need to be protected during the interim period?

5. How will the development of the grid to accommodate the interconnection of future renewable generation affect the resilience of the grid to attack? Will the presence of future additional renewable generation itself add to or detract from the resilience of the grid to physical attack?

6. What are the obstacles to developing a more resilient grid? What strategies can be used to address these obstacles?

a. Cost?

b. Siting?

c. Regulatory Barriers?

d. Staffing/training?

Panelists:

- Ken Seiler, PJM Interconnection
- Tracy McCrory, Tennessee Valley Authority
- Daniel Sierra, Burns and McDonnell

Closing Remarks (4:10–4:30 p.m.)

[FR Doc. 2023–16474 Filed 8–1–23; 8:45 am]

BILLING CODE 6717–01–P