ORAL ARGUMENT NOT YET SCHEDULED

No. 20-1247

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

UNION OF CONCERNED SCIENTISTS,

Petitioner,

v.

UNITED STATES DEPARTMENT OF ENERGY,

Respondent.

On Petition for Review of Orders
of the U.S. Department of Energy

BRIEF OF *AMICI CURIAE* AMERICAN PUBLIC POWER ASSOCIATION, THE EDISON ELECTRIC INSTITUTE, THE LARGE PUBLIC POWER COUNCIL, AND THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION IN SUPPORT OF RESPONDENT AND AFFIRMANCE

DELIA PATTERSON
JOHN E. MCCAFFREY
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
dpatterson@publicpower.org
jmccaffrey@publicpower.org

EMILY S. FISHER
ROBERT STROH
EDISON ELECTRIC INSTITUTE
701 Pennsylvania Ave., NW
Washington, DC 20004
(202) 508-5000
EFisher@eei.org
RStroh@eei.org

JONATHAN D. SCHNEIDER
STINSON LLP
1775 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com

NICHOLAS J. PASCALE
NATIONAL RURAL ELECTRIC
COOPERATIVE ASSOCIATION
4301 Wilson Blvd.
Arlington, VA 22203
703-907-5557
nicholas.pascale@nreca.coop

Counsel for Large Public Power Council

Dated: January 15, 2021

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), amici curiae include this certificate as to parties, rulings, and related cases.

A. Parties and Amici. All parties and amici appearing before the United States Department of Energy and in this Court appear in the Brief for Petitioner.

B. Rulings Under Review. An accurate reference to the rulings under review appears in the Brief for Petitioner.

C. Related Cases. An accurate statement regarding related cases appears in the Brief for Petitioner.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 28(a)(1) and Circuit Rules 26.1 and 28(a)(1)(A), amici curiae make the following disclosures:

The American Public Power Association ("APPA") has no parent corporation or publicly traded stock.

The Edison Electric Institute ("EEI") is an incorporated, not-for-profit national trade association. EEI has no parent corporation, and no publicly held corporation holds a 10 percent or greater ownership interest in EEI.

The Large Public Power Council ("LPPC") has no parent corporation or publicly traded stock.

The National Rural Electric Cooperative Association ("NRECA") has no parent corporation or publicly traded stock.

INTERESTS OF AMICI CURIAE

Pursuant to Federal Rule of Appellate Procedure 29(a) and Circuit Rule 29(b), and in accordance with Federal Rule of Appellate Procedure 29(a)(6), Circuit Rule 29(c), and the briefing schedule issued by the Court on September 29, 2020 (as modified by the Court's November 23, 2020 order), APPA, EEI, LPPC, and NRECA (collectively, "Electric Trade Associations") filed a *Notice of Intent to Participate as Amicus Curiae* on January 4, 2020. As stated in that *Notice*, the Electric Trade Associations certify that all parties in this appeal have consented to the Electric Trade Associations filing this brief *amici curiae* in support of Respondent, the U.S. Department of Energy.

APPA is the national service organization representing the interests of not-for-profit, state, municipal, and other locally owned electric utilities throughout the United States. More than 2,000 public power utilities provide over 15 percent of all kilowatt-hour sales to ultimate customers and to businesses in every state except Hawaii.

EEI is an association that represents all U.S. investor-owned electric companies. EEI's members provide electricity for about 220 million Americans and operate in all 50 states and the District of Columbia. EEI regularly files amicus curiae briefs in cases raising issues of concern to its members.

LPPC is the association of the 27 largest state-owned and municipal utilities in the nation. Located throughout the nation, LPPC's members comprise the larger, asset-owning utilities in the public power community, owning approximately 90 percent of the transmission assets owned by non-federal public power entities. LPPC members are also members of APPA.

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landscape. Electric cooperatives operate at cost and without a profit incentive.

An important function of each of the Electric Trade Associations is to represent the interests of their respective members in matters before Congress, the Executive Branch, federal agencies, and the courts. No party to this case authored this brief in whole or in part. No party and no person other than the Electric Trade Associations funded or contributed funding for the preparation of this brief.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Statutes

Regulations

Other Authorities

*Authorities upon which we chiefly rely are marked with asterisks.

GLOSSARY

APPA	American Public Power Association
CEII	Critical Electric Infrastructure Information
Department	U.S. Department of Energy
EEI	Edison Electric Institute
Electric Trade Associations	American Public Power Association, Edison Electric Institute, Large Public Power Council, and National Rural Electric Cooperative Association
FERC	Federal Energy Regulatory Commission
Final Rule	*Critical Electric Infrastructure Information; New Administrative Procedures*, Final Rule, 85 Fed. Reg. 14,756 (Mar. 16, 2020)
FOIA	Freedom of Information Act
LPPC	Large Public Power Council
NRECA	National Rural Electric Cooperative Association

INTRODUCTION

Petitioner Union of Concerned Scientists challenges a final rule issued by the U.S. Department of Energy ("Department") that provides clarity regarding how the Department will designate critical electric infrastructure information ("CEII") and protect CEII from inappropriate disclosure. *Critical Electric Infrastructure Information; New Administrative Procedures, Final Rule*, 85 Fed. Reg. 14,756 (Mar. 16, 2020) (the "Final Rule"). CEII is a type of critical infrastructure information explicitly exempted from disclosure under the Freedom of Information Act ("FOIA") by Congress in 2015. Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003, 129 Stat. 1312, 1773-79 (2015) (codified at 16 U.S.C. §824*o*-1). Congress exempted CEII from FOIA and state and local public records laws so that this highly sensitive information could not be used to compromise critical electric infrastructure and "negatively affect national security, economic security, public health or safety, or any combination of such matters." 16 U.S.C. § 824*o*-1(a)(2); *see also* 16 U.S.C. § 824*o*-1(d)(1). The Department's rules for designating and protecting CEII from disclosure are lawful, reasonable and consistent with Congress' intent to protect such information from disclosure, as explained in detail in Respondent Department's brief.

Petitioner asks the Court to overturn the Department's reasonable and lawful rules based in part on the suggestion that the Department overstates the security

implications of disclosing CEII. *See* Pet. Br. at 24 (dismissing the Final Rule's restrictions on sharing CEII as based on "vague platitudes about national security"). Petitioner maintains, in fact, that the Final Rule's restrictions on release of CEII could threaten the security of the electric grid. *See*, *e.g.*, Pet. Br. at 5 (asserting that "the Department's restrictions [on sharing CEII] will make those [electrical] systems less secure, and less reliable"); *id.* at 24 (arguing that the Final Rule's "sweeping and unexplained restrictions on sharing information newly constrain beneficial access to information, creating threats to security, safety, reliability, and emergency preparedness"); *id.* at 49 (asserting that "the Department's failure to consider the countervailing costs of overly broad claims that information is CEII, and the real public harms—including to safety, security, and reliability—of mislabeling and restricting the flow of information among nonfederal entities is arbitrary and capricious"). In suggesting that the Department overstates or misjudges the security concerns associated with sharing CEII, Petitioner misconstrues the nature of CEII, how it could be used to harm electric reliability, and why Congress explicitly exempted it from disclosure. These security concerns are real and legitimate and have been recognized across the federal government.

The members of the Electric Trade Associations are owners and operators of the nation's electric grid, which comprises three distinct functions: generation and storage, transmission, and distribution. As such, they are the source of much of the

CEII that would be submitted (mostly voluntarily) to the Department under its rules. They also are charged with—and legally obligated to provide for—the safety and security of the nation's electric infrastructure. The nation's electric utilities take these obligations to provide affordable, safe, reliable, and resilient electricity to all customers seriously. Electric companies take a risk-based "defense-in-depth" approach to protecting critical energy grid assets and systems from threats. This multi-layered approach encompasses compliance with rigorous, mandatory, and enforceable reliability and cybersecurity standards and regulations, and includes activities that surpass the minimum requirements; close coordination within the industry and with government partners at all levels; and efforts to prepare, respond, and recover should an incident impact the electric grid. Accordingly, the Electric Trade Associations and the members they represent are best positioned to provide necessary background on the real threats facing the critical infrastructure that is the electric grid and the importance of ensuring that the CEII that Congress clearly intended to protect from disclosure is so protected.

ARGUMENT

I. The Risk of Cyberattacks Against the Nation's Critical Electric Infrastructure is Real; Disclosure of CEII Increases These Risks.

The electric grid is resilient, capable of recovering quickly from damage to its components or the external systems on which it depends. Electric Trade Associations' members work quickly to respond to adverse consequences from any

incident that impacts reliability to restore power expeditiously to the customers who depend on reliable electricity. While members are highly qualified and exceptional at responding to and recovering from disaster-related events, like hurricanes, other storms, and wildfires, physical and cyberattacks present unique challenges and the potential for resulting outages. Protecting critical infrastructure information is essential to protect against these consequences.

The risk of cyberattack on electric grid assets, in particular, has become an urgent concern in recent years, increasing the need to ensure that information that could facilitate such an attack is kept out of the hands of malicious actors. Federal agencies and the owners and operators of critical infrastructure, including electric infrastructure, are dependent on information technology systems to carry out essential functions. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being. Accordingly, information security is recognized as an area of high-risk by the federal government. *See* Government Accountability Office, High Risk Series, Urgent Actions are Needed to Address Cybersecurity Challenges Facing the Nation, GAO-18-622 (Sept. 2018), https://www.gao.gov/assets/700/694355.pdf.

With its focus on seeking greater access to protected CEII (or narrowing the scope of information that should be classified as CEII), Petitioner minimizes the real and legitimate threats posed to the nation's critical electric infrastructure by those

who would do us harm and the role that access to CEII could play in facilitating that harm. Understanding these real risks and how access to critical information increases them is essential for any consideration of Petitioner's suggestion that the Department misjudged the risks associated with designating, protecting, and sharing CEII.

The threat that cyberattacks pose to electric infrastructure and the damage that such attacks could cause not only to that infrastructure but to the entire U.S. economy is well-recognized. The capabilities and sophistication of hostile forces seeking to attack the U.S. electric grid and destabilize the nation increases continually. *See* Government Accountability Office, Critical Infrastructure Protection, Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid, GAO-19-332, at 16 (Aug. 2019), https://www.gao.gov/assets/710/701079.pdf. The Government Accountability Office, in synthesizing various reports on the cybersecurity threat posed to electric infrastructure, notes that nations, criminal groups, and terrorists pose the most significant threats, followed by hackers and hacktavists, as well as insiders. *See id.* at 17-21. According to the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community, China and Russia pose the greatest cyberattack threat and could cause localized, temporary disruptions of critical infrastructure. For example, Russia has the ability to disrupt an electric distribution network for at least a few hours and is mapping U.S. critical

infrastructure with the goal of being able to cause more substantial damage. This Assessment also states that Iran is attempting to deploy cyberattack capabilities that would enable attacks against critical infrastructure, and that North Korea retains the ability to conduct disruptive cyberattacks. *See* Daniel R. Coats, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, testimony before the Senate Select Committee on Intelligence, 116th Cong. 1st sess., Jan. 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

These cyberattack capabilities are not inchoate. In 2018, the Federal Bureau of Investigation and the Department of Homeland Security publicly revealed that a foreign nation-state engaged in a prolonged, "multi-stage intrusion campaign" against U.S. electric utilities. *See* United States Computer Emergency Readiness Team (US-CERT), Alert TA18-074A, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (Mar. 16, 2018), https://www.uscert.gov/ncas/alerts/TA18-074A. In addition, in 2018, the Department of Justice indicted foreign hackers who successfully penetrated hundreds of U.S. institutions. In releasing the indictment, the Department of Justice specifically cited the grave risk posed by malicious actors targeting the U.S. electric sector and noted that the attackers had targeted the Federal Energy Regulatory Commission ("FERC") because it had access to critical electric infrastructure

information. *See Daniel Voltz*, *U.S. charges, sanctions Iranians for global cyber attacks on behalf of Tehran*, REUTERS (Mar. 23, 2018), https://www.reuters.com/article/us-usa-cyber-iran/u-s-charges-sanctions-iranians-for-global-cyber-attacks on-behalf-of-tehran-idUSKBN1GZ22K.

The Department's CEII regulations protect sensitive information that could help these attackers succeed in their efforts. Making this information public, or sharing it too widely, could assist malicious actors seeking to attack U.S. electric infrastructure. Even seemingly benign information can present real cybersecurity risks depending on the context in which it is disclosed. Information as basic as the name of a particular utility, when coupled with other publicly available information, could provide would-be attackers with information that would allow them to better target their efforts. In late 2020, in recognition of the fact that different pieces of information, coupled with CEII, could be used by malicious parties to their advantage, FERC staff adopted additional protections for certain CEII that it has in its possession. *See* Second Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards, Docket No. AD19-18-000 (Sept. 23, 2020), https://www.ferc.gov/media/second-joint-staff-white-paper-notices-penalty-pertaining-violations-critical-infrastructure. In further limiting access to CEII, FERC staff noted that this revised approach was necessary because of the "tangible risks" of making such information public and that such risks

necessitate a higher level of protection, consistent with the CEII protections provided by Congress. *See id.* at 2, 4.

Attackers are creative and endlessly innovative; they can use new information in a variety of ways, particularly if they have already begun "mapping" our electric system. In light of these risks, the Department's Final Rule, appropriately and consistent with FOIA, restricts the disclosure and sharing of sensitive information relating to critical electric infrastructure, and, in particular, reasonably limits sharing of CEII with non-federal entities to situations where "the release of information is in the national security interest." 10 C.F.R. § 1004.13(j)(2) (2020).

II. Undermining the Exemption for CEII Would Undermine the Vital Public-Private Partnership That Protects the Electric Grid.

In the Final Rule, the Department recognizes that, unlike FERC, most of the CEII that could be in its possession would be provided voluntarily. *See* 85 Fed. Reg. at 14,757. FERC receives significant amounts of CEII through its regulatory and enforcement functions. The Department, in contrast, is not primarily a regulatory agency; it plays an essential role in an important public-private partnership established by the federal government to protect critical electric infrastructure. Accordingly, any differences between the Department's and FERC's CEII regulations (which are more similar than not) are at least partially a function of their different roles.

As a preliminary matter, it is important to understand the role that the Department plays in protecting critical electric infrastructure. Presidential Policy Directive 21, issued in February 2013, shifted the nation's focus from protecting critical infrastructure against terrorism to protecting and securing this infrastructure and increasing its resilience against all hazards, including cyber incidents. *See* White House, Presidential Policy Directive 21/PPD-21: Critical Infrastructure Security and Resilience, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. This Directive identified 16 critical infrastructure sectors, including the energy sector, which includes the electric grid. *See id.* The Directive also designated the Department as the sector-specific agency for the energy sector and charged the Department with collaborating with critical infrastructure owners and operators to identify vulnerabilities and mitigate incidents. *See id.* The Department's sector-specific role was codified in the Fixing America's Surface Transportation Act of 2015, the same law that exempted CEII from disclosure under the Freedom of Information Act. *See* Pub. L. No. 114-94, Div. F, § 61003(a), 16 U.S.C. § 824*o*-1(b).

The National Infrastructure Protection Plan, which was updated by the Department of Homeland Security in 2013, further integrated the critical infrastructure protection efforts of the federal government and the private sector

owners of this infrastructure. It describes a voluntary partnership model as the mechanism for coordinating these efforts. *See* Department of Homeland Security, National Infrastructure Protection Plan, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (Dec. 2013), https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. As part of this partnership, the Department, as the designated sector-specific agency, serves as the lead coordinator for the federal government's security programs for the energy sector. The Department leads these efforts through the Energy Sector Coordinating Council and, more specifically, the Electricity Subsector Coordinating Council, which includes representatives from the Electric Trade Associations' members. A key goal of these efforts is to expand and improve the sharing of information related to cyber threat indicators, defensive measures, and other cybersecurity information, as these measures mitigate risks. As the sector-specific agency for the energy sector, the Department creates programs to enhance the cybersecurity of energy infrastructure and engages in certain voluntary data collection and analysis programs to promote energy security and the resilience of U.S. energy infrastructure, in support of national security.

Because most CEII that may be provided to the Department will be done so voluntarily, a lack of adequate protection against disclosure of such information could disincentivize Electric Trade Associations' members from providing such

information to the Department. As the owners and operators of the electric grid, they have a legal obligation to ensure the grid's reliability, which is enforceable. *See* 16 U.S.C. § 824*o*(e). Electric Trade Associations' members also take their obligations to their customers to provide affordable, reliable, and resilient power seriously. Eliminating or weakening the protection from disclosure afforded CEII that is provided by the Final Rule not only would make information potentially available to would-be attackers, but also would erode the public-private partnership that strives to better protect the energy grid from attack.

CONCLUSION

Petitioner seeks to overturn the Department's regulations addressing the designation and protection of critical electric infrastructure information. Such information, if not protected from disclosure, could be used by would-be attackers, and the threat of such outcomes is real and documented. Moreover, eroding the Department's ability to protect such information from disclosure will harm the public-private partnership that the federal government relies on to protect critical infrastructure, largely through information sharing. Electric Trade Associations' members may be discouraged from such information sharing if the risk of public disclosure or sharing with non-federal entities is too great. Both of these outcomes should be avoided as they would harm critical infrastructure protection and be

inconsistent with Congress's goals in protecting CEII from disclosure in the first place.

Respectfully submitted,

s/ John E. McCaffrey
DELIA PATTERSON
JOHN E. MCCAFFREY
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
dpatterson@publicpower.org
jmccaffrey@publicpower.org

s/ Emily S. Fisher
EMILY S. FISHER
ROBERT STROH
EDISON ELECTRIC INSTITUTE
701 Pennsylvania Ave., NW
Washington, DC 20004
(202) 508-5000
EFisher@eei.org
RStroh@eei.org

s/ Jonathan D. Schneider
JONATHAN D. SCHNEIDER
STINSON LLP
1775 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com

Counsel for Large Public Power Council

s/ Nicholas J. Pascale
NICHOLAS J. PASCALE
NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION
4301 Wilson Blvd.
Arlington, VA 22203
703-907-5557
nicholas.pascale@nreca.coop

Dated: January 15, 2021

CERTIFICATE OF COMPLIANCE WITH RULE 32(g)

I hereby certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 2,341 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f) and Circuit Rule 32(e)(1).

I further certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. 32(a)(6) because it has been prepared in 14-point Times New Roman, a proportionally spaced typeface, using Microsoft Word 2016.

By: */s/ John E. McCaffrey*

JOHN E. MCCAFFREY
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
jmccaffrey@publicpower.org

ADDENDUM

ADDENDUM
TABLE OF CONTENTS

§ 824*o*-1. Critical electric infrastructure security

(a) Definitions

For purposes of this section:

. . . .

(2) Critical electric infrastructure

The term "critical electric infrastructure" means a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters.

. . . .

(b) Authority to address grid security emergency

(1) Authority

Whenever the President issues and provides to the Secretary a written directive or determination identifying a grid security emergency, the Secretary may, with or without notice, hearing, or report, issue such orders for emergency measures as are necessary in the judgment of the Secretary to protect or restore the reliability of critical electric infrastructure or of defense critical electric infrastructure during such emergency. As soon as practicable but not later than 180 days after December 4, 2015, the Secretary shall, after notice and opportunity for comment, establish rules of procedure that ensure that such authority can be exercised expeditiously.

(2) Notification of Congress

Whenever the President issues and provides to the Secretary a written directive or determination under paragraph (1), the President shall promptly notify congressional committees of relevant jurisdiction, including the Committee on Energy and Commerce of the House of Representatives and the Committee on Energy and Natural Resources of the Senate, of the contents of, and justification for, such directive or determination.

(3) Consultation

Before issuing an order for emergency measures under paragraph (1), the Secretary shall, to the extent practicable in light of the nature of the grid security emergency and the urgency of the need for action, consult with appropriate governmental authorities in Canada and Mexico, entities described in paragraph (4), the Electricity Sub-sector Coordinating Council, the Commission, and other appropriate Federal agencies regarding implementation of such emergency measures.

(4) Application

An order for emergency measures under this subsection may apply to—

(A) the Electric Reliability Organization;

(B) a regional entity; or

(C) any owner, user, or operator of critical electric infrastructure or of defense critical electric infrastructure within the United States.

(5) Expiration and reissuance

(A) In general

Except as provided in subparagraph (B), an order for emergency measures issued under paragraph (1) shall expire no later than 15 days after its issuance.

(B) Extensions

The Secretary may reissue an order for emergency measures issued under paragraph (1) for subsequent periods, not to exceed 15 days for each such period, provided that the President, for each such period, issues and provides to the Secretary a written directive or determination that the grid security emergency identified under paragraph (1) continues to exist or that the emergency measure continues to be required.

(6) Cost recovery

(A) Critical electric infrastructure

If the Commission determines that owners, operators, or users of critical electric infrastructure have incurred substantial costs to comply with an order for emergency measures issued under this subsection and that such costs were prudently incurred and cannot reasonably be recovered through regulated rates or market prices for the electric energy or services sold by such owners, operators, or users, the Commission shall, consistent with the requirements of section 824d of this title, after notice and an opportunity for comment, establish a mechanism that permits such owners, operators, or users to recover such costs.

(B) Defense critical electric infrastructure

To the extent the owner or operator of defense critical electric infrastructure is required to take emergency measures pursuant to an order issued under this subsection, the owners or operators of a critical defense facility or facilities designated by the Secretary pursuant to subsection (c) that rely upon such infrastructure shall bear the full incremental costs of the measures.

(7) Temporary access to classified information

The Secretary, and other appropriate Federal agencies, shall, to the extent practicable and consistent with their obligations to protect classified information, provide temporary access to classified information related to a grid security emergency for which emergency measures are issued under paragraph (1) to key personnel of any entity subject to such emergency measures to enable optimum communication between the entity and the Secretary and other appropriate Federal agencies regarding the grid security emergency.

. . . .

(d) Protection and sharing of critical electric infrastructure information

(1) Protection of critical electric infrastructure information

Critical electric infrastructure information--

(A) shall be exempt from disclosure under section 552(b)(3) of Title 5; and

(B) shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision or tribal law requiring public disclosure of information or records.

. . . .

§ 824*o*. Electric Reliability

. . . .

(e) Enforcement

(1) The ERO may impose, subject to paragraph (2), a penalty on a user or owner or operator of the bulk-power system for a violation of a reliability standard approved by the Commission under subsection (d) if the ERO, after notice and an opportunity for a hearing—

(A) finds that the user or owner or operator has violated a reliability standard approved by the Commission under subsection (d); and

(B) files notice and the record of the proceeding with the Commission.

(2) A penalty imposed under paragraph (1) may take effect not earlier than the 31st day after the ERO files with the Commission notice of the penalty and the record of proceedings. Such penalty shall be subject to review by the Commission, on its own motion or upon application by the user, owner or operator that is the subject of the penalty filed within 30 days after the date such notice is filed with the Commission. Application to the Commission for review, or the initiation of review by the Commission on its own motion, shall not operate as a stay of such penalty unless the Commission otherwise orders upon its own motion or upon application by the user, owner or operator that is the subject of such penalty. In any proceeding to review a penalty imposed under paragraph (1), the Commission, after notice and opportunity for hearing (which hearing may consist solely of the record before the ERO and opportunity for the presentation of supporting reasons to affirm, modify, or set aside the penalty), shall by order affirm, set aside, reinstate, or modify the penalty, and, if appropriate, remand to the ERO for further proceedings. The Commission shall implement expedited procedures for such hearings.

(3) On its own motion or upon complaint, the Commission may order compliance with a reliability standard and may impose a penalty against a user or owner or operator of the bulk-power system if the Commission finds, after notice and opportunity for a hearing, that the user or owner or operator of the bulk-power system has engaged or is about to engage in any acts or practices that constitute or will constitute a violation of a reliability standard.

(4) The Commission shall issue regulations authorizing the ERO to enter into an agreement to delegate authority to a regional entity for the purpose of proposing reliability standards to the ERO and enforcing reliability standards under paragraph (1) if—

(A) the regional entity is governed by—

(i) an independent board;

(ii) a balanced stakeholder board; or

(iii) a combination independent and balanced stakeholder board.

(B) the regional entity otherwise satisfies the provisions of subsection (c)(1) and (2); and

(C) the agreement promotes effective and efficient administration of bulk-power system reliability.

The Commission may modify such delegation. The ERO and the Commission shall rebuttably presume that a proposal for delegation to a regional entity organized on an Interconnection-wide basis promotes effective and efficient administration of bulk-power system reliability and should be approved. Such regulation may provide that the Commission may assign the ERO's authority to enforce reliability standards under paragraph (1) directly to a regional entity consistent with the requirements of this paragraph.

(5) The Commission may take such action as is necessary or appropriate against the ERO or a regional entity to ensure compliance with a reliability standard or any Commission order affecting the ERO or a regional entity.

(6) Any penalty imposed under this section shall bear a reasonable relation to the seriousness of the violation and shall take into consideration the efforts of such user, owner, or operator to remedy the violation in a timely manner.

. . . .

§ 1004.13 Critical electric infrastructure information.

. . . .

(j) Sharing of CEII—

. . . .

(2) Non-federal Entities. The Secretary or the CEII Coordinator shall make a final determination whether to share CEII materials requested by non-federal entities that are within the categories specified in section 215A(d)(2)(D) of the FPA. A request by such a non-federal entity shall not be entertained unless the requesting non-federal entity demonstrates that the release of information is in the national security interest and it has entered into a Non–Disclosure Agreement with DOE that ensures, at a minimum:

(i) Use of the information only for authorized purposes and by authorized recipients and under the conditions prescribed by the Secretary or CEII Coordinator;

(ii) Protection of the information in a secure manner to prevent unauthorized access;

(iii) Destruction or return of the information after the intended purposes of receiving the information have been fulfilled;

(iv) Prevention of viewing or access by individuals or organizations that have been prohibited or restricted by the United States or the Department from viewing or accessing CEII;

(v) Compliance with the provisions of the Non–Disclosure Agreement, subject to DOE audit;

(vi) No further sharing of the information without DOE's permission; and

(vii) CEII provided pursuant to the agreement is not subject to release under the Freedom of Information Act, 5 U.S.C. 552(b)(3), and shall not be made available by any Federal, state, political subdivision, or tribal authority pursuant to any Federal, State, political subdivision, or tribal law requiring public disclosure of information or records pursuant to sections 215A(d)(1)(A) and (B) of the Federal Power Act.

(viii) The Non–Disclosure Agreement must state that the agreement applies to all subsequent releases of CEII during the calendar year in which the DOE and the non-federal entity enter into the agreement. As a result, the non-federal entity will not be required to file a Non–Disclosure Agreement with subsequent requests during the calendar year.

. . . .

CERTIFICATE OF SERVICE

Pursuant to Rule 25(d) of the Federal Rules of Appellate Procedure, I hereby certify that on January 15, 2021, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ John E. McCaffrey
John E. McCaffrey
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
jmccaffrey@publicpower.org