UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Indicated ISO/RTOs	**)**	**Docket Nos. AD26-___-000**
Indicated Transmission Owners	**)**	**RM26-___-000**

PETITION FOR RULEMAKING REGARDING IMPROVEMENTS TO PROTECTIONS FOR CRITICAL ENERGY/ELECTRIC INFRASTRUCTURE INFORMATION

In accordance with Rule 207 of the Federal Energy Regulatory Commission's ("Commission") Rules of Practice and Procedure,[1] the indicated Independent System Operators and Regional Transmission Organizations ("ISOs/RTOs")[2] and Commission-jurisdictional transmission-owning utilities[3] (together, "Petitioners") respectfully request that the Commission address increasing cyberthreats by improving its protections for both: (i) "Critical Energy/Electric Infrastructure Information" held or generated by the Commission under 18 C.F.R. § 388.113; and (ii) sensitive electric infrastructure information pertaining to Commission-jurisdictional facilities shared by non-governmental entities, such as ISOs/RTOs and other jurisdictional transmission providers that is outside the scope of § 388.113 but commonly referred to as CEII. Both types of information are referred to as "CEII" throughout this petition. In particular, while CEII protections attach to information submitted to or released by the Commission, the existing regulations do not

[1] 18 C.F.R. § 385.207 (2026).

[2] The ISO/RTO petitioners are the Alberta Electric System Operator ("AESO"); the Independent Electricity System Operator ("IESO") of Ontario; ISO New England Inc. ("ISO-NE"); Midcontinent Independent System Operator, Inc. ("MISO"); New York Independent System Operator, Inc. ("NYISO"); and Southwest Power Pool, Inc. ("SPP"). Although the AESO and IESO are not subject to the Commission's jurisdiction, they join these comments to express support.

[3] The transmission-owning utility petitioners are Central Hudson Gas & Electric Corporation; Consolidated Edison Company of New York, Inc.; Niagara Mohawk Power Corporation d/b/a National Grid; the New York Power Authority, New York State Electric & Gas Corporation; Orange & Rockland Utilities, Inc.; Rochester Gas & Electric, and Tucson Electric Power Company.

apply to information exchanged between ISOs/RTOs and between ISOs/RTOs and their stakeholders.

Action is needed to address the increasing amounts of sensitive information shared by ISOs/RTOs and other non-governmental entities. The need is growing because of intensifying threats to critical infrastructure and proliferating requests for information about it. Robust measures are essential to ensure confidence that such information will remain protected when shared by ISOs/RTOs, market participants, and other authorized users, such as parties requesting interconnection or transmission service, consultants, and researchers. The Commission should explore adding more detailed requirements to the non-disclosure agreements ("NDAs") executed by CEII recipients to provide stronger and more uniform protection, and to clarify if and how these protections are to apply to earlier-created documents related to the CEII received. Many entities are subject to a patchwork of inconsistent and limited information protection requirements. These inconsistencies can be problematic, for example, when one ISO's/RTO's information safeguards are undermined by weaker protections in neighboring regions. The Commission should also evaluate whether its regulations should be strengthened to reinforce, and to avoid subverting, more stringent safeguards that may be adopted by ISOs/RTOs and others.

Petitioners propose that the Commission begin by convening a technical conference, or by issuing a Notice of Inquiry and inviting written comments, or by taking an alternative procedural approach that the Commission deems appropriate to build a record. The Commission should then proceed to a notice-and-comment rulemaking to consider the improvements recommended. In particular, the Commission should explore developing new *pro forma* tariff provisions or agreements, such as an updated and strengthened NDA. The Commission could also clarify various questions that ISOs/RTOs frequently encounter, including: (i) when CEII designations

should attach to data; (ii) how information not designated as CEII by the Commission but still requiring comparable protection should be treated; (iii) if there should be mechanisms for ISOs/RTOs and other transmission providers to seek guidance from federal CEII Coordinators; and (iv) whether there are categories of information that should receive greater protection than CEII does today. The Commission should also be open to proposed improvements that may be advanced by other parties.

The Commission should also, as it has always done when formulating critical infrastructure information rules, carefully balance the need for security improvements against the potential for undue impediments to information access.

Any action initiated in response to this petition would not implicate the President's directive to eliminate regulations under Executive Order 14192, *Unleashing Prosperity Through Deregulation* ("Unleashing Prosperity EO").[4] New measures to enhance CEII protections should be eligible for the Unleashing Prosperity EO's exception for "regulations issued with respect to a . . . national security, or homeland security . . . related function of the United States." Taking the actions proposed herein would also be consistent with President Trump's recently issued *Cyber Strategy for America*.[5]

I. THE NEED FOR COMMISSION ACTION

Starting with a policy statement issued shortly after the September 11, 2001 attacks,[6] the Commission has established various requirements to define, protect, and govern access to CEII.[7]

---

[4] 90 Fed. Reg. 9065 (Feb. 6, 2025).

[5] *See* THE WHITE HOUSE, PRESIDENT TRUMP'S CYBER STRATEGY FOR AMERICA (2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf ("Cyber Strategy for America").

[6] *See e.g., Statement of Policy on Treatment of Previously Public Documents*, 66 Fed. Reg. 52917 (Oct. 18, 2001), 97 FERC ¶ 61,130 (2001).

[7] *See Critical Energy Infrastructure Information*, Order No. 630, 102 FERC ¶ 61,190, *order on reh'g*, Order No. 630-A, FERC Stats. & Regs. 104 FERC ¶ 61,106 (2003); *Amendments to Conform Regulations With Order No.*

Over the years, the Commission has made changes to clarify the rules, address emerging concerns, and respond to statutory directives. The Commission's efforts to date are codified at 18 C.F.R. § 388.113 (the "CEII Protection Rule").

The Commission has not updated the CEII Protection Rule since 2016 when it issued Order No. 833 in response to the Fixing America's Surface Transportation Act ("FAST Act").[8] That statute added Section 215A to the Federal Power Act ("FPA") to "improve the security and resilience of energy infrastructure in the face of emergencies."[9]

Petitioners recognize the vital importance of safeguarding CEII and other highly sensitive information regarding Critical Electric Infrastructure. They are already working diligently to reduce threats of improper disclosure. But there are limits to what ISOs/RTOs, and utilities, as non-governmental entities, can achieve independently or through voluntary coordination. The Commission should therefore take the lead by initiating proceedings to consider new protections for the exchange of CEII and CEII-like data by ISOs/RTOs and other non-governmental entities, stronger NDA requirements, and other potential improvements. A reassessment of CEII protections, and Commission action to adopt appropriate enhancements, is warranted to stay ahead of emerging threats.

---

630 (Critical Energy Infrastructure Information Final Rule), Order No. 643, 68 Fed. Reg. 52089 (Sept. 2, 2003); *Critical Energy Infrastructure Information*, Order No. 649, 108 FERC ¶ 61,121 (2004); *Critical Energy Infrastructure Information*, Order No. 662, 70 Fed. Reg. 37031 (June 28, 2005); *Critical Energy Infrastructure Information*, Order No. 683, 116 FERC ¶ 61,263 (2006), *order on reh'g*, Order No. 683-A, 119 FERC ¶ 61,029 (2007); *Critical Energy Infrastructure Information*, Order No. 702, 121 FERC ¶ 61,107 (2007); *Regulations Implementing FAST Act Section 61003 – Critical Electric Infrastructure Security and Amending Critical Energy Infrastructure Information*, Order No. 833, 157 FERC ¶ 61,123, (2016). *See also* Critical Energy/Electric Infrastructure Information (CEII) Regulations, FERC, https://www.ferc.gov/major-orders-regulations/critical-energyelectric-infrastructure-information-ceii-regulations.

[8] Order No. 833, 157 FERC ¶ 61,123.

[9] Order No. 833 at P 5.

A. There Are Gaps in Current CEII Protections

Under the CEII Protection Rule, the Commission, its employees, and its contractors have a duty to protect CEII,[10] including information concerning Critical Electric Infrastructure.[11] The current regulation also specifies procedures for accessing CEII[12] and sanctions for knowingly making unauthorized disclosures.[13]

However, FPA Section 215A's definition of "Critical Electric Infrastructure Information" expressly applies only to information "generated by or provided to the Commission or other Federal agency[.]"[14] Accordingly, Order No. 833 recognized that "because the CEII designation only applies to information that is submitted to or generated by the Commission, information that Commission staff accesses and reviews, but never takes custody of, cannot be designated as CEII."[15] At the same time, the Commission suggested that information that was outside the scope of the CEII definition could still "be treated as non-public information" and "be afforded the same treatment as CEII."[16]

FPA Section 215A directed the Commission to "issue regulations aimed at securing and sharing sensitive information."[17] This included a requirement to facilitate "voluntary sharing of critical electric infrastructure information with, between, and by . . . owners, operators, and users

---

[10] 18 C.F.R. § 388.113(h).

[11] § 388.113(c)(3) ("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.").

[12] § 388.113(g).

[13] § 388.113(i).

[14] 16 U.S.C. § 824o-1(a)(3).

[15] Order No. 833 at P 56.

[16] *Id*. at P 57.

[17] *Id*. at P 5.

of critical electric infrastructure in the United States . . ."[18] In the rulemaking that preceded Order No. 833, two ISO/RTO commenters asked the Commission to facilitate the sharing of CEII by ISOs/RTOs and other entities with Commission-approved tariffs or other agreements establishing their own information handling requirements. The Commission denied this request on the ground that "existing non-public voluntary sharing mechanisms within the energy industry are sufficient to encourage sharing information among the different groups and therefore that there is no need for the Commission to establish requirements for sharing within the industry through tariff revisions or otherwise."[19] But the Commission also indicated that it had discretion to "identify, encourage, and support existing processes to facilitate the voluntary sharing of CEII."[20]

The Commission has authority beyond FPA Section 215A to build on the currently effective CEII Protection Rule. For example, the Commission issued the original version of its CEII rules in 2003 based on its general authority under the FPA and the Natural Gas Act.[21] The Commission has stated that ISOs/RTOs and other jurisdictional transmission providers have discretion to craft CEII protections appropriate to their individual circumstances.[22] The Commission could also look to the Electric Reliability Council of Texas, Inc. ("ERCOT"), which has adopted an ERCOT-specific definition of CEII, i.e., "ECEII" that is modeled on, but not identical to, the Commission's definition.[23] ECEII encompasses sensitive information developed by ERCOT itself.

---

[18] 16 U.S.C. § 824o-1(d)(2)(D).

[19] Order No. 833 at P 122.

[20] *Id.* at n.196.

[21] *See* Order No. 630, 102 FERC ¶ 61,190 at P 5 ("The Commission is issuing this rule under the authority of the Federal Power Act and the Natural Gas Act . . . ." (citing 15 U.S.C. 717, *et seq*.; 16 U.S.C. 791, *et seq*.)).

[22] *See e.g., Midwest Indep. Transmission Sys. Operator, Inc*., 123 FERC ¶ 61,1164 at P 35 (2008).

[23] *See e.g*., Nodal Protocol Revision Request (NPRR) 902, ERCOT Critical Energy Infrastructure Information.

While CEII is subject to the Commission's protections when it is in the Commission's hands, it is also frequently exchanged, often pursuant to Commission requirements, without the same safeguards among ISOs/RTOs, market participants, developers, transmission and interconnection customers, and other individuals with a valid need-to-know. This often occurs before entities designate the information as CEII or before a designation is accepted by the Commission. The absence of standard protections for CEII and potential CEII in such instances allows for inconsistent regional practices that may not always be sufficient to protect critical infrastructure from increasing threats.

In addition, the current CEII process could be clearer as to how the Commission will determine what information concerning Critical Electric Infrastructure it will designate as CEII. Individual submitters are left to justify their requests that submitted information be treated as CEII based on limited guidance on the Commission's website.[24] Submissions are then reviewed on their case-specific merits by one of the Commission's CEII Coordinators.[25] CEII Coordinators' reliance on the analyses and justifications offered by individual parties, rather than a coherent and uniform standard, can result in inconsistent designations and greater risks of improper disclosures.

Furthermore, the Commission's current protections are principally implemented through various standardized NDA forms.[26] The current version of the Commission's General NDA imposes some disclosure restrictions as well as some security obligations that are based on the

[24] *See* 18 C.F.R. § 388.113(d)(1)(i). *See also* CEII Filing Guide, FERC, https://www.ferc.gov/ceii-filing-guide.

[25] 18 C.F.R. § 388.113(d)(1)(v).

[26] *See* 18 C.F.R. § 388.113(g)(5). *See also* CEII Overview, FERC, Critical Energy/Electric Infrastructure Information (CEII)| Federal Energy Regulatory Commission (providing the option to select and execute either the Commission's General NDA, Media NDA, Federal Agency Acknowledgement and Agreement, State Agency Employee NDA, or Consultant NDA), https://www.ferc.gov/enforcement-legal/ceii/electronic-ceii-request-form.

National Institute of Science and Technology ("NIST") SP 800-171.[27] It would be helpful if the NDA established more detailed information protection and cybersecurity requirements applicable to all recipients. In addition, the current General NDA does not require any affirmative verification or attestation by an officer confirming that the NDA's requirements are being implemented.

In 2020, the Eastern Interconnection Planning Collaborative ("EIPC") urged the Commission to revise FERC Form 603, i.e., the CEII request form.[28] The EIPC raised concerns similar to those of the Petitioners here. The EIPC argued that Form 603 did "not provide adequate protection against the release of CEII" and that Form 603's requirements were "insufficient to guard against transmission related CEII falling into the wrong hands."[29] More specifically, "Form 603 would allow for access to certain highly confidential information embodied in Parts 2, 3, and 6 of FERC Form 715."[30] The EIPC argued that, while Form 715 data may not have been sufficient to help malicious actors plan attacks in the past, "given the advancement of technology and proliferation of cyber attack information, such data could allow vulnerabilities of the bulk power system to be exploited leading to widespread damage and prolonged loss of service."[31] The Commission did not make any changes to Form 603 in response to the EIPC's requests. The Petitioners believe that the EIPC's concerns continue to be valid and further support Petitioners' view that the time has come to explore potential improvements to the CEII NDAs.

---

[27] *See* Critical Energy/Electric Infrastructure Information Non-Disclosure Agreement at ¶ 9, n.1, https://www.ferc.gov/sites/default/files/2025-12/CEII%20General%20NDA%20.pdf.

[28] *See Comments of the Eastern Interconnection Planning Collaborative*, Docket No. IC20-13-000 (May 8, 2020) ("EIPC Comments").

[29] *Id.* at 1, 2.

[30] *Id.* at 2.

[31] *Id*.

ISOs/RTOs have some ability to create more stringent and detailed protections for CEII and other information on their own. Some ISOs/RTOs have already done so. However, broader and stronger protections established through new *pro forma* tariff provisions or agreements would be a more effective and consistent way to close protection gaps. Even if individual ISOs/RTOs were to secure the Commission's approval of regional information protection proposals under FPA Section 205, they cannot establish nationally consistent protections themselves. And creating parallel frameworks to address gaps in coverage for the same data without updating the CEII rules themselves is likely to cause confusion. Given the increasing threats discussed below, the Commission should consider whether the time has come to reinforce its own CEII NDA. Any concern that new *pro forma* requirements might lack sufficient flexibility could be addressed by allowing entities to obtain regional variations under the "consistent with or superior to" standard.

B. Two Significant Trends Highlight the Need to Strengthen CEII Protections

Two major trends are driving the need for enhanced protection of CEII. Namely, cyber threats are growing in number and severity while the number of requests for CEII is increasing.

First, the North American Electric Reliability Corporation ("NERC") has repeatedly warned that the "threat landscape includes continuously evolving and persistent threats from sophisticated, capable, and diverse adversaries," including from "nation states, which possess the capability to disrupt critical infrastructure in North America."[32] NERC highlighted the ongoing evolution and intensification of cyber threats in its comments regarding the Commission's October 2025 reliability technical conference:

> The threat environment for both cyber and physical attacks continues to evolve, with greater potential for coordinated, hybrid events targeting operational

[32] *Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid: Hearing Before the Subcomm. on Energy of the H. Comm. on Energy & Com*., 119th Cong. (2025) (written testimony of Michael Ball, Chief Executive Officer, Electricity Information Sharing & Analysis Center & Sr. Vice President, NERC, at 10), https://d1dth6e84htgma.cloudfront.net/12_02_2025_ENG_Testimony_Ball_d7d714c179.pdf.

> technology (OT) systems. Safeguarding our grid from adversaries and their cyber and physical attacks is a constant concern. New technologies used on the grid for supply and transmission create new vectors for exploitation, and harmful actors change, evolve, and grow in sophistication.[33]

A review of recent cybersecurity incidents illustrates the increasing risk of unauthorized disclosures of sensitive information. Since 2020, several widespread cybersecurity incidents have successfully targeted software used by many businesses and the federal government. For example, in 2022, hackers targeted Sargent & Lundy, a prominent engineering firm and government contractor focused on power and energy generation that works on critical infrastructure projects nationwide. Along with other sensitive information, the breach exposed transmission data and model files pertaining to various utility projects. Although the Sargent & Lundy breach was reportedly contained, similar attacks could create catastrophic security risks. "[S]ecurity experts have long been concerned that schematics held by electric and nuclear power contractors could be dumped online and used for follow-on physical or cyberattacks on those facilities."[34]

Similarly, the 2023 "MOVEit" cyberattack targeted transfer software used by hundreds of organizations, resulting in data being stolen from many businesses and government agencies, and the 2020 SolarWinds cyberattack incident impacted software used by thousands of private and government parties. The energy sector has also been the target of attacks on individual companies that have had wide-ranging impacts on critical infrastructure. A well-documented example is the 2021 Colonial Pipeline ransomware attack. That intrusion forced the company to shut down all of

[33] North Am. Elec. Reliability Corp., Pre-Conference Comments, Docket No. AD25-8-000, at 6-7 (filed Oct. 21, 2025).

[34] *See* Sean Lyngaas, *Hackers stole data from multiple electric utilities in recent ransomware attack*, CNN POLITICS (Dec. 27, 2022), https://www.cnn.com/2022/12/27/politics/hackers-data-utilities-ransomware-sargent-lundy.

its pipelines, resulted in emergency declarations in eleven states, and triggered panic-buying that caused gasoline shortages.

In addition, state-sponsored cyberattacks against utility infrastructure are frequently in the news and have prompted warnings by domestic cybersecurity agencies.[35] On April 7, 2026, the Cybersecurity and Infrastructure Security Agency issued an advisory concerning ongoing efforts by "Iranian-affiliated advanced persistent threat actors" to exploit internet-connected operational technology devices in order to target critical infrastructure in the energy, water, and other industries.[36] The Transportation Security Administration warned in February that "[r]ecent coordinated strikes against Iran and retaliatory missile attacks targeting U.S. and Israeli interests have increased the potential for threats to the homeland, including cyberattacks, acts of violence, and hate crimes."[37] The President's *Cyber Strategy for America* also states that it is a national cyber "policy pillar" to "Secure Critical Infrastructure" which necessitates an effort to "identify, prioritize, and harden America's critical infrastructure and secure its supply chains, including . . . the energy grid . . . ."[38] Taking the actions recommended in this petition is consistent with this Presidential directive.

Industry-wide and targeted attacks both pose significant risks to Critical Electric Infrastructure which are further amplified by the risk of improper disclosure of CEII. There is

---

[35] *See, e.g.*, Cybersecurity & Infrastructure Security Agency, Alert: Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps, (Feb. 10, 2026), https://www.cisa.gov/news-events/alerts/2026/02/10/poland-energy-sector-cyber-incident-highlights-ot-and-ics-security-gaps.

[36] Cybersecurity & Infrastructure Security Agency, Cybersecurity Advisory: Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across U.S. Critical Infrastructure, (Apr. 7, 2026), https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a.

[37] Ben Lefebvre, Myah Ward, & Mike Soraghan, *DHS warns US energy companies to beef up security for possible Iranian retaliation*, E&E NEWS BY POLITICO, (Mar. 4, 2026), https://subscriber.politicopro.com/article/2026/03/homeland-security-warns-us-energy-companies-to-beef-up-security-for-possible-iranian-retaliation-00810691.

[38] *Cyber Strategy for America* at 5.

every reason to anticipate that further attacks by criminal organizations or hostile governmental actors will become more common and more sophisticated in the future, particularly with the advent of artificial intelligence ("AI") and agentic AI. Recent reports regarding the power of new AI tools to defeat even the strongest cybersecurity measures are especially alarming.[39] Even individual disclosures that appear low-risk may compound as the cumulative volume of improperly disclosed data is subject to advanced analytic techniques.

Second, an increase in generation and transmission project development activity has materially increased the number of requests for CEII,[40] with a commensurate expansion in the scope of potential risks. For example, in July 2024, the Federal Bureau of Investigation's Cyber Division released a Private Industry Notification warning of the heightened risk of cyberattacks associated with the renewable energy industry's growth.[41] This trend is also likely to accelerate in the future for multiple reasons, most notably expectations of enormous load growth attributable to data centers. As the Department of Energy stated in its October 2025 Advanced Notice of Proposed Rulemaking on large load interconnections, "United States electricity demand is expected to grow at an extraordinary pace, due, in large part, to the rapid growth of large loads . . . Although there are several drivers to this demand growth, such as home and vehicle electrification, increasing quantities of large commercial and industrial load, most notably data centers, are connecting rapidly to the transmission system."[42]

---

[39] *See, e.g.* Amrith Ramkumar, Robert McMillan, & Katherine Blunt, *White House Officials Discuss Assessing AI Models That Pose Security Risks*, THE WALL STREET JOURNAL (May 4, 2026), https://www.wsj.com/tech/ai/white-house-officials-discuss-assessing-ai-models-that-pose-security-risks-5c9e4b9e.

[40] For example, the NYISO has processed between 1,421 and 2,461 CEII requests per year over the past few years, mainly in connection with new interconnection requests.

[41] Federal Bureau of Investigation – Cyber Division, Private Industry Notification No. 20240701-001: Expansion of US Renewable Energy Industry Increases Risk of Targeting by Malicious Cyber Actors (July 1, 2024).

[42] Advanced Notice of Proposed Rulemaking, Docket No. RM26-4-000, at P 1 (filed Oct. 27, 2025).

Many participants in the electric utility industry already have stringent security practices in place to comply with NERC's mandatory Critical Infrastructure Protection ("CIP") standards. However, there may be some developers and consultants supporting developers not subject to the CIP standards. And no matter how much security certain parties may maintain to protect CEII, all facilities and facility owners are at risk if others do not have comparable safeguards. Given the worsening threat environment, it is timely for the Commission to reevaluate and to consider strengthening CEII protections.

II. POTENTIAL IMPROVEMENTS TO CEII PROTECTIONS

Petitioners' preliminary view is that the Commission should prioritize the development of new *pro forma* tariff provisions and agreements to address the sharing of CEII among ISOs/RTOs and other entities, including transmission owners, market participants, transmission and interconnection customers, consultants, and researchers. Because the CEII Protection Rule applies only to information submitted to or generated by the Commission, but development and aggregation of such information often require the exchange of the information with other entities, there is a need to create uniform protections for other situations. Petitioners are not proposing specific changes to regulatory text in the Code of Federal Regulations at this time. Petitioners do not foresee any need to alter the existing regulatory definition of "Critical Energy/Electric Infrastructure Information." But the Commission may wish to adopt additional, complementary, regulatory language to implement particular improvements.

The Commission should establish safeguarding requirements for recipients of CEII provided by an ISO/RTO or other non-governmental entity that uniformly apply to all recipients to ensure equal treatment for all parties and a consistent level of security for this information. For example, new *pro forma* language could require CEII recipients to verify or attest that they meet and are in fact implementing specific security standards such as authentication protocols, access

control, password practices, encryption, security updates, data sanitation, physical security standards, supply chain protections, workforce management protections and security incident disclosure requirements. As noted above, the existing CEII NDA does not include such a verification or attestation requirement. Moreover, the Commission's procedures lack clarity as to continuing compliance and enforcement. Members of the public who receive CEII through the Commission's process are not asked to demonstrate compliance with data protection protocols nor periodically certify that such procedures remain in place. Adopting such verification and attestation standards for all CEII recipients would: (i) provide assurance commensurate with increasing threat levels that all sensitive information will be protected regardless of who is asked to provide it; and (ii) facilitate and expedite the effective review of increasing numbers of CEII requests. Adding a verification or attestation requirement could also facilitate enforcement of the CEII NDA by strengthening the Commission's ability to sanction CEII recipients that are not Commission-jurisdictional entities.[43]

Pro forma provisions could also establish requirements for all entities seeking to share CEII to ensure uniformity. Protections today can vary across different regions. Certain types of sensitive information, such as power flow cases, tend to contain detailed information regarding facilities located outside of a transmission provider's geographic footprint. Thus, even if a transmission provider were to impose heightened security requirements on itself, the same power flow information could be obtained from a neighboring entity with lesser security requirements.

[43] CEII recipients that fail to comply with the CEII NDA's terms may lose their ability to appear before the Commission and acknowledge that they may be subject to civil or criminal sanctions under Sections 316A or 316(b) of the FPA. *See* CEII NDA, §18. Those FPA provisions apply to any "person." Adding a verification or attestation requirement could reinforce the Commission's ability to impose sanctions on "persons" that are not otherwise Commission-jurisdictional. Various ISOs/RTOs use verification or attestation requirements in non-CEII-related market rules for similar reasons. *See, e.g.*, NYISO Services Tariff, Section 23.4.5.7.9.2.1 (establishing certification requirements for officers of entities applying for a "competitive entry" exemption from capacity market mitigation measures).

Bilateral NDAs could partially address this concern, but relying on them is inefficient as parties must negotiate every request. Standardized NDAs would also be more readily enforceable.

Subject to future record-building and rulemaking proceedings, the Commission could establish *pro forma* provisions that would impose enhanced protection requirements to receive CEII held by non-government entities. These enhanced requirements could be guided by the NIST SP 800-171 standards currently incorporated in the Commission's General NDA for CEII. The Commission might also make use of alternatives to the NIST rules, such as the ISO/IEC 27001 information security standards, if the Commission determines that they are more suitable for certain categories of information and their use is consistent with existing law.

The EIPC has adopted a voluntary NDA that is available to all NERC-registered Planning Coordinators and Transmission Planner organizations that are located within, or adjacent to, the Eastern Interconnection. This Planning Coordinator/Transmission Planner ("PCTP") NDA was designed to streamline and facilitate the exchange of CEII. The PCTP NDA was first established to address Order No. 1000 and NERC MOD-032 requirements, which necessitated the exchange of significant amounts of data and information deemed to be CEII. EIPC recently updated the agreement to account for coordination requirements under Order Nos. 1920 and 2023 that involve CEII exchanges.[44] The Commission should consider the PCTP NDA's terms when exploring potential improvements to its own General NDA and CEII rules, including whether it could take steps to reinforce the PCTP NDA or similar efforts.[45]

---

[44] *See* Memorandum from John P. Buechler, EIPC Executive Director, on CEII Sharing Non-Disclosure Agreement to Eastern Interconnection Planning Coordinators & Transmission Planners (Feb. 19, 2025) (available at: *https://eipconline.com/s/MemorandumfromExecutiveDirectorreUpdatedPCTPNDA5-1-25.pdf; https://eipconline.com/s/FINAL-EIPC-PCTP-CEII-NDA-Rev-2-19-25.pdf*).

[45] For example, under the PCTP NDA, the CEII rules of the entity whose data is being requested governs requests from third parties even if such data is also in the possession of a neighboring transmission provider.

Furthermore, the Commission should evaluate its procedures for processing third-party requests for access to CEII. Certain ISOs/RTOs have received notice of third-party requests for CEII access that have not adequately been justified, but the Commission has dismissed those ISOs/RTOs' objections summarily. The Commission should require individuals requesting CEII access from the Commission to provide more detailed information justifying their requests. The Commission should also require CEII applicants to utilize relevant ISO/RTO or other transmission provider CEII procedures before seeking such information from the Commission. By encouraging (if not requiring) this sequencing, the Commission could serve in more of an appellate capacity should a member of the public be aggrieved by an ISO/RTO or transmission provider's action on its request.

The Commission could also address various CEII-related questions that ISOs/RTOs often face, but which presently lack answers. For example, when should a CEII designation attach to data? At present, a CEII designation applies to documents prepared by or submitted to the Commission or other federal agencies. Stakeholders often do not inform ISOs/RTOs exactly what they want to designate as CEII until shortly before a filing. But a great deal of sensitive information often changes hands before a filing is made. Relatedly, how should transmission providers treat information that they receive that is not designated as CEII but which they believe warrants comparable protection? Are there situations in which transmission providers should be permitted to request that the information they produce receive CEII-like protection? And should this protection apply to information that has the hallmarks of CEII but which may not necessarily ever be submitted to the Commission?[46] When, if ever, should a CEII designation be removed

[46] For example, some of the information included with regional planning or generator interconnection studies is identical to information that would be labelled "CEII" if it were submitted to the Commission.

before the expiration of the five-year period specified in the Commission's regulations, for example, if information becomes sufficiently aggregated or de-identified?

Similarly, the current CEII Protection Rule empowers the Commission's CEII Coordinators to decide what constitutes CEII and when it may be released. Will ISOs/RTOs and other transmission providers need to retain similar personnel to fulfill new responsibilities to protect CEII? Should there be a process for transmission providers to seek guidance from the CEII Coordinators regarding when they should protect and when they should release such information? Or should transmission providers be empowered to perform certain functions of a CEII Coordinator for information that they generate or possess?

In addition, except for a few administrative requirements, a CEII designation does not offer any more protection than that provided to other types of confidential information (beyond more severe consequences for unauthorized exposure). There is thus an incentive for parties to propose "confidential" treatment even when they potentially should be asking for a CEII designation, so as to receive a similar degree of protection with reduced exposure to sanctions. The Commission should consider how to address this issue, which might involve establishing a heightened level of information protection beyond what CEII designations provide today. For example, ERCOT has a "Super ECEII" concept that accounts for different types of ECEII potentially involving different levels of security risk. ERCOT has discretion to restrict access to ECEII or to remove otherwise required ECEII postings on the secure portion of ERCOT's website, if ERCOT determines that the information poses a high level of security risk.[47]

[47] ERCOT Nodal Protocols, §1.3.2.(4) ("Different types of ECEII may involve different levels of security risk. In its discretion, ERCOT may restrict Market Participant access to ECEII created or received by ERCOT that poses a high level of security risk . . ." subject to certain requirement, and "If ERCOT determines that ECEII that is required to be posted on the ERCOT website or MIS Secure Area pursuant to these Protocols or an Other Binding Document poses a high level of security risk, ERCOT shall remove such information from the ERCOT website or MIS Secure Area notwithstanding such posting requirement, . . .").

As the Commission has long recognized, it will be necessary to balance the need for greater information protections with the need to maintain efficient access to CEII for parties with a valid reason to access it. It will likewise be important to avoid unduly burdening ISOs/RTOs and other entities that handle voluminous amounts of sensitive information. Stronger and more consistent requirements will generally be beneficial. But timely access to CEII is also essential to certain tasks that involve frequent and time-sensitive information requests as resource utilization and transmission planning, where it is common and necessary to share information with many stakeholders and their consultants. In addition, timely access to CEII is necessary for educational and other research institutions to conduct important research projects that seek to improve the security, reliability, and efficiency of the bulk-power system. Excessively stringent protections could unintentionally become harmful barriers to entry and innovation if they impede decisions regarding the development of interconnection and transmission facilities or if they restrain research and development projects. The notice-and-comment rulemaking proceedings requested in this petition will help the Commission to find the right balance.[48]

III. THE COMMISSION SHOULD CONVENE A TECHNICAL CONFERENCE OR ALTERNATIVE PROCEDURES TO EXPLORE THE ISSUES RAISED HEREIN AND THEN PROCEED TO INITIATE A RULEMAKING TO IMPROVE CEII PROTECTIONS

The Commission could begin by holding a technical conference to gather additional input from industry leaders and enable stakeholders to offer their perspectives. Petitioners expect that the record developed at such a conference, together with the information presented in this petition,

[48] The Commission and parties should also be mindful of the potential implications of extending protections to information about Critical Electric Infrastructure held outside the government. Overlaps between the Commission's CEII requirements and the National Archives and Records Administration's regulations regarding Controlled Unclassified Information could have complex and unexpected consequences, including for contractors in the electricity sector. While these issues are important, Petitioners respectfully submit that the Commission does not need to resolve them before beginning reform efforts.

will provide a more than sufficient evidentiary basis to justify initiating a notice-and-comment rulemaking. As discussed above, Petitioners have preliminary views regarding the reforms that the Commission should pursue. But other participants' perspectives should also be heard.

This approach would be similar to the one that the Commission successfully followed in Docket Nos. AD20-6 and RM22-13 preceding the issuance of Order No. 895. Those proceedings began with the Commission convening a technical conference to discuss principles and best practices for credit risk management in organized wholesale electric markets.[49] The Commission then issued a Notice of Proposed Rulemaking[50] and reviewed parties' comments. In the end, the Commission promulgated Order No. 895, which directed ISOs/RTOs to adopt tariff provisions to authorize the sharing of credit-related information regarding market participants.[51] That information-sharing framework could be a model for new, uniform protections governing the sharing of CEII by and among ISOs/RTOs and others.

Alternatively, the Commission could begin with a Notice of Inquiry or take another procedural approach that it believes would be more efficient or effective to develop a record. The most important thing is for the Commission to begin the process of addressing the issues presented by this petition.

IV. IMPROVING PROTECTIONS FOR CEII WILL STRENGTHEN NATIONAL AND HOMELAND SECURITY AND THUS SHOULD NOT TRIGGER THE REQUIREMENTS OF THE UNLEASHING PROSPERITY EXECUTIVE ORDER

Petitioners are mindful that the President of the United States has prioritized reducing regulatory burdens through the Unleashing Prosperity EO and other measures, which discourage

[49] *Credit-Related Information Sharing in Organized Wholesale Electric Markets*, Order No. 895, 183 FERC ¶ 61,193 at P 8 (2023).

[50] *Id.* at P 10.

[51] *Id*.

the introduction of new regulations. However, the actions that Petitioners are asking the Commission to take are consistent with the President's priorities and should be permissible without any need to eliminate other regulations. They are also consistent with the priority that the President has placed on securing critical infrastructure in the *Cyber Strategy for America*.

The Unleashing Prosperity EO generally requires that whenever a federal agency "publicly proposes for notice and comment or otherwise promulgates a new regulation, it shall identify at least 10 existing regulations to be repealed." But there is an important exception: any regulation that is "issued with respect to a . . . national security, [or] homeland security . . . related function of the United States" is exempt from the "10-for-1" repeal requirement. Although the Commission is not principally a national security agency, enhancing protections for CEII would unquestionably support the national security and homeland security functions of the United States.

The FAST Act expressly identified "Critical Electric Infrastructure" as "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." The Commission's current CEII framework was "designed to limit the distribution of sensitive infrastructure information to those individuals with a need to know in order to avoid having sensitive information fall into the hands of those who may use it to attack the Nation's infrastructure."[52] The FAST Act is clear that protecting CEII is a matter of national security. Improving these protections would also be consistent with the President's emphasis on addressing a declared national energy emergency and supporting the development of artificial

[52] Order No. 833 at P 4.

intelligence data centers.[53] In short, the Commission should not be required to eliminate other regulations if it takes the actions requested by this petition.

V. CONCLUSION AND COMMUNICATIONS

The electricity sector in the United States is facing rapidly evolving and ever more complex cybersecurity threats at a time when requests for CEII are proliferating. Petitioners respectfully ask the Commission to consider new protections for the sharing of CEII, additional NDA requirements for CEII recipients, and other potential enhancements to safeguards for sensitive CEII and CEII-like data. For all of the foregoing reasons, Petitioners respectfully request that the Commission schedule a technical conference or alternative record-building procedures and then initiate a rulemaking to explore such measures.

Petitioners respectfully ask that all pleadings, correspondence and other communications filed in this proceeding should be addressed to each of the signatories below.

Respectfully submitted,

/s/ Ted J. Murphy
Ted J. Murphy
Hunton Andrews Kurth LLP

Counsel for the New York Independent System Operator, Inc.

June 2, 2026

[53] Exec. Order No. 14141, 90 Fed. Reg. 11 (Jan. 17, 2025); Exec. Order No. 14156, 90 Fed. Reg. 8433 (Jan. 29, 2025); Exec. Order No. 14179, 90 Fed. Reg. 20 (Jan. 31, 2025); Exec. Order No. 14365, 90 Fed. Reg. 239 (Dec. 16, 2025).

/s/ Gillian Barnett, LLB Gillian Barnett (she/her), LLB Vice President, Law and Customer Projects, General Counsel & Corporate Secretary 3000, 240 – 4th Avenue SW Calgary, Alberta, Canada T2P 4H4 403-512-9932 Gillian.Barnett@aeso.ca *General Counsel for Alberta Electric System Operator (AESO)*	/s/ *Amber Martin Stone* Amber Martin Stone Senior FERC Counsel AVANGRID NETWORKS, INC. 180 Marsh Hill Road Orange, CT 06477 475-318-1876 amber.stone@avangrid.com *Attorney for New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation*
/s/ Christopher R. Sharp Christopher R. Sharp Associate General Counsel Central Hudson Gas & Electric Corporation 284 South Avenue Poughkeepsie, NY 12601 845-486-2000 csharp@cenhud.com	*/s/ Mary Krayeske* Mary Krayeske Assistant General Counsel Consolidated Edison Company of New York, Inc and Orange and Rockland Utilities, Inc. 4 Irving Place – 18-801 New York, NY 10003 917-647-8052 krayeskem@coned.com
/s/ Michael Boll Michael Boll General Counsel and Corporate Secretary Independent Electricity System Operator (IESO) 120 Adelaide Street West, Suite 1600, Toronto, ON, M5H 1T1 416-969-6023 Michael.Boll@ieso.com	/s/ *Maria Gulluni* Maria Gulluni Vice President, General Counsel and Chief Compliance Officer ISO New England Inc. One Sullivan Road Holyoke, MA 01040-2841 413-540-4473 MGulluni@iso-ne.com
/s/ Christopher D. Supino Christopher D. Supino Managing Senior Corporate Counsel Midcontinent Independent System Operator, Inc. 720 City Center Drive Carmel, IN 46032 317-249-5256 csupino@misoenergy.org *Counsel for the Midcontinent Independent System Operator, Inc.*	*/s/ Amber Thornhill* Amber Thornhill Director, FERC and ISO Relations & Market Policy National Grid 801 Pennsylvania Ave., N.W. Suite 801 Washington, DC 20004 215-696-6689 Amber.Thornhill@nationalgrid.com

/s/ Robert E. Fernandez Robert E. Fernandez, Executive Vice President, Chief Compliance Officer & General Counsel New York Independent System Operator, Inc. 10 Krey Boulevard Rensselaer, NY 12144 518-356-6000 rfernandez@nyiso.com	/s/ *Eric Rotfeld* Eric Rotfeld Special Counsel New York Power Authority 123 Main Street White Plains, New York 10601 914-390-8025 / 914-574-7173 eric.rotfeld@nypa.gov
/s/ *Tessie Kentner* Tessie Kentner Associate General Counsel Southwest Power Pool, Inc. 201 Worthen Drive Little Rock, AR 72223 501-482-2436 tkentner@spp.org *Attorney for* *Southwest Power Pool, Inc.*	/s/ *Sarah Meadows* Sarah Meadows Sr. Attorney Tucson Electric Power Company 88 E. Broadway Tucson Arizona, 85701 520-734-0959 sarah.meadows@tep.com

cc: Janel Burdick
Emily Chen
James Dawson
Jignasa Gadani
Leanne Khammal
Jaime Knepper
David Morenoff
Jason Rhee
Douglas Roe