CRITICAL ENERGY / ELECTRIC INFRASTRUCTURE INFORMATION
GENERAL NON-DISCLOSURE AGREEMENT

1. These provisions govern the use of Critical Energy/Electric Infrastructure Information (CEII) provided to an individual who files a request for access to CEII pursuant to 18 C.F.R. § 388.113.

2. Definitions - For purposes of these provisions:

> **a.** The term "CEII Coordinator" refers to the Federal Energy Regulatory Commission (Commission) official designated as the CEII Coordinator, with delegated authority under 18 C.F.R. § 375.313 to make determinations with respect to requests for CEII and make determinations as to whether information fits within the definition of CEII.
>
> **b.** The terms "non-disclosure agreement" and "NDA" mean this agreement by which requesters certify their understanding that access to CEII is provided pursuant to the terms and restrictions of these provisions, and that such requesters have read the provisions and agree to be bound by them.
>
> **c.** The term "Recipient" means someone who is approved to receive CEII in accordance with the provisions of 18 C.F.R. § 388.113.

3. A Recipient may only discuss CEII with another authorized Recipient of the identical CEII. A Recipient may check with the CEII Coordinator to determine whether another individual is an authorized Recipient of the identical CEII.

4. If any Recipient submits information to the Commission that includes CEII obtained under these provisions, the portions of the filing containing CEII must be submitted in accordance with 18 C.F.R. § 388.113(d)(1).

5. A Recipient of CEII may use CEII as foundation for advice provided to others but may not disclose CEII to another individual unless that individual is an authorized Recipient of the identical CEII.

6. A Recipient may only use CEII for the purpose for which it was requested and must not use CEII for an illegal or illegitimate purpose.

7. All CEII shall be maintained by the Recipient in a secure place in a manner that conforms with industry standards, such as those specified by the National Institute of Standards and Technology (NIST), to prevent unauthorized electronic or physical access[1], and only made accessible to other authorized Recipients of the identical CEII. Within 5 business days of a request from Commission staff, the Recipient will provide details on the Recipient's methods of securely maintaining and safeguarding CEII.

8. Recipients may make copies of CEII, but such copies of CEII are subject to the restrictions specified herein. Recipients may make notes concerning CEII, which shall be subject to the

restrictions herein if such notes contain CEII.

9. A Recipient must notify the Commission of any unauthorized disclosure of CEII or any data breach or other security incident that may involve Commission provided CEII within two business days of the data breach or knowledge thereof, and the recipient agrees to provide the Commission an incident management report describing Recipient's response to the data breach and all corrective action that has or will be taken within 5 business days.

10. CEII provided pursuant to the agreement is not subject to release under either the Freedom of Information Act or other Sunshine Laws.

11. Recipients must return CEII to the CEII Coordinator or destroy CEII within fifteen days of a written request by the CEII Coordinator to do so, except that CEII notes may be retained in accordance with Paragraph 7, above. Within such time period, each Recipient, if requested to do so, shall also submit to the CEII Coordinator an affidavit stating that, to the best of his or her knowledge, all CEII has been returned or destroyed and that CEII notes have either been returned, destroyed or are being maintained by Recipient in accordance with Paragraph 7.

12. The Recipient is obligated to protect the CEII, even after designation period has lapsed, until the CEII Coordinator determines the information should no longer be designated as CEII under 18 C.F.R. § 388.113(e)(2), or a court of competent jurisdiction finds that the information does not qualify as CEII.

13. The Recipient must promptly notify the Commission if any conditions, such as a change in employment, have occurred.

14. The Commission may audit the Recipient's compliance with this non-disclosure; agreement, and Recipient agrees to fully cooperate with the Commission in any compliance monitoring and auditing processes.

15. I hereby certify my understanding that access to CEII is provided to me pursuant to the terms and restrictions of the above provisions, that I have been given a copy of and have read the provisions, and that I agree to be bound by them. I understand that the contents of the CEII, any notes or other memoranda, or any other derivative form of information that copies or discloses CEII shall not be disclosed to anyone other than another person who has been granted access to these same materials by the Commission.

16. If Recipient fails to comply with any of the provisions of this Agreement, the Commission reserves the right to suspend Recipient's ability to appear before the Commission pursuant to 18 C.F.R. § 385.2102 and may require the immediate destruction or return of the information, as well as taking any other legally available action. To that end, Recipient acknowledge that a violation of this non-disclosure agreement may result in criminal sanctions (including a fine of up to $25,000 per day per offense pursuant to Section 316(b) of the Federal Power Act, 16 U.S.C. § 825o(b)), or civil sanctions under Section 316A of the Federal Power Act, 16 U.S.C. § 825o-1.

[1] See NIST Special Publication (SP) 800-171“Protecting CUI in Nonfederal Systems and Organizations” and 800-172 “Enhanced Security Requirements for Protecting Controlled Unclassified Information - A Supplement to NIST Special Publication 800-171”. A summary of NIST security requirements 3.8.1 through 3.8.9 are attached hereto as Appendix A. Compliance measures include access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection and system and information integrity.

Appendix A

NIST Basic Security Requirements and Derived Security Requirements

Basic Security Requirements:

- 3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
- 3.8.2 Limit access to CUI on system media to authorized users.
- 3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

Derived Security Requirements:

- 3.8.4 Mark media with necessary CUI markings and distribution limitations.
- 3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
- 3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- 3.8.7 Control the use of removable media on system components.
- 3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.
- 3.8.9 Protect the confidentiality of backup CUI at storage locations.

Name:

Title:

Representing:

Email Address:

Signature: