WECC
Electric Reliability and Security for the West

Entity CEII Guidance
WECC Enforcement
1 March 2019

The North American Electric Reliability Corporation (NERC) files information with the Federal Energy Regulatory Commission (FERC) regarding enforcement dispositions and/or settlement of violations of NERC Reliability Standards. Some information from those filings may be made publicly available when approved by FERC. FERC has recently emphasized that a registered entity, the Regional Entity, and NERC should not assume that information in a disposition or settlement, because it relates to Critical Infrastructure Protection (CIP) or Emergency Preparedness and Operations (EOP), will automatically be considered confidential or exempt from a Freedom of Information Act (FOIA) request filed with FERC.

Appendix 4C, Section 9.3.3, of the NERC Rules of Procedure (ROP) states, "[i]nformation deemed to be Critical Energy Infrastructure Information shall be redacted, in accordance with Section 1500 of the NERC [ROP], and shall not be released publicly." As an interested party, the entity may use the provisions of the ROP to help it identify and protect Critical Energy/Electric Infrastructure Information (CEII). Part of this process includes marking CEII for redaction and giving a justification for the nondisclosure of confidential/non-public information in the face of a FOIA request.

WECC gives entities this document as guidance when identifying CEII. This resource can help entities as they mark documents for redaction and write the justification for requesting confidential/non-public protection of any CIP or EOP disposition or settlement public filing. This guide is not meant to provide legal advice but is merely one resource among other resources an entity may consult in protecting its information. Some other resources are listed below.

CEII Definitions and FOIA Guidance

FERC's CEII Definitions:

FERC provides some helpful guidance related to CEII on its website:

> CEII is defined as information related to or proposed to critical electric infrastructure,
>
> - generated by or provided to the Commission or other Federal agency other than classified national security information,
> - that is designated as critical electric infrastructure information by the Commission or the Secretary of the Department of Energy pursuant to section 215A(d) of the Federal Power Act.

CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

1. Relates details about the production, generation, transmission, or distribution of energy;
2. Could be useful to a person planning an attack on critical infrastructure;
3. Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552 (2000); and
4. Does not simply give the general location of the critical infrastructure.

Critical energy/electric infrastructure means a system or asset of the bulk-power system, (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.

For more information, see https://www.ferc.gov/legal/ceii-foia/ceii.asp?csrt=13257659154056985275.

U.S. DOJ FOIA Guidance:

Anyone may refer to the United States Department of Justice Guide to the Freedom of Information Act (Guide), which is a comprehensive legal treatise on the FOIA. The Guide includes detailed discussions of the FOIA's procedural requirements, nine exemptions, and litigation considerations. Each section contains a detailed analysis of the key judicial opinions issued on the FOIA.

For more information, see https://www.justice.gov/oip/doj-guide-freedom-information-act-0.

CEII Justification Categories

NERC and the Regional Entities compiled a list of 12 high-level categories for information that is generally considered CEII and/or non-public and often redacted from the public filing of CIP and EOP dispositions and settlements.

1. BES Cyber System Information, including security procedures;
   - Information related to BES Cyber Assets;
   - Details of Electronic Security Perimeter diagrams that include BES Cyber Asset names, BES Cyber System names, individual IP addresses with context and/or group(s) of IP addresses;
   - IP addresses, IP address ranges;
   - Security information or names, that are not publicly available, regarding BES Cyber Assets, BES Cyber Systems, Protected Cyber Assets, Physical Access Control Systems, Electronic Access Control and Monitoring Systems; and

- Network topology diagrams, Physical Security Perimeter diagrams, and related information.

2. The names of the entity's vendors and contractors.
3. The names and NERC Compliance Registry numbers of the registered entity.
4. The registered functions and registration dates of the registered entity.
5. The names of entity facilities.
6. The names of entity assets.
7. The names of entity employees.
8. The names of departments that are unique to the entity.
9. The sizes and scopes of the entity's operations.
10. The dates of Compliance Audits of the entity, as those dates may have been included in schedules published by the Regional Entities.
11. The dates of Self-Reports submitted while preparing for Compliance Audits.
12. The NERC Violation ID of prior instances of noncompliance.

General Process for Redaction and Justification

WECC will provide to the entity, via its Enhanced File Transfer (EFT) server, a PDF of the public version of the disposition or settlement filing.

After getting the file, the entity should mark for redaction—b**ut not apply the redaction**—to any CEII content. The entity must use Adobe Acrobat Pro to mark the PDF for redaction. If that is not available, the entity should highlight the information it requests to be redacted. For all marked information, the entity should provide a justification and a length of time for which the CEII confidential/non-public protection should remain in place.

NERC has recommended CEII confidential/non-public protection for three to five years for Category 1 redactions (BES Cyber System Information-specific redactions), and, for Categories 2 through 12 (information that could identify the entity), two to three years as long as the noncompliance is mitigated and up to five years if the noncompliance is not yet mitigated.

For any requests not included in the 12 categories, the entity should provide justification for the request and how long the information should be protected. After review, the entity should return to WECC, via the EFT server, the marked documents with justifications.

WECC asks that entities return their requests within:

- Five business days for a Compliance Exception (CE); and

- 10 business days for a Find, Fix, Track, and Report (FFT), Settlement Agreement, or Notice of Confirmed Violations (NOCV).

WECC follows time constraints imposed by the NERC ROP, FERC Rules of Practice and Procedure[1], and FOIA. If the entity does not respond within the timeframe, WECC will assume the entity has no input on the matter. If the entity is unable to meet the timeframe, it may request an extension of time from WECC to complete the task.

In addition to an entity's review, WECC may perform its own review of each CIP and EOP filing and make its own request for CEII confidential/non-public protection. This may expand, reduce, or replace the entity's request. This will be based upon the reasonableness of the entity's request, justification provided, or direction from NERC or FERC. NERC makes the final decision on all requests for CEII confidential/non-public protection before filing with FERC.

For questions, please contact Heather Laws, Director of Enforcement, at hlaws@wecc.org or 801-819-7642.

[1] See generally *Title 18, Code of Federal Regulations, Part 385*, et al.