Justification for CEII Treatment

For the reasons discussed below, NERC is providing a redacted version of its Compliance Exceptions, Find, Fix, Track and Report issues (FFT), and Spreadsheet Notices of Penalty (SNOP) pursuant to Sections 39.7(b)(4) and 388.113 of the Commission's regulations. NERC respectfully requests that the Commission designate the redacted portions of the Compliance Exceptions, FFTs, and SNOPs as non-public and as Critical Energy/Electric Infrastructure Information ("CEII"), consistent with Sections 39.7(b)(4) and 388.113. This request for non-public and CEII treatment applies to all CIP Compliance Exceptions and FFTs posted by NERC and SNOPs submitted by NERC. Justifications that are specific to each noncompliance will be included in an accompanying document.

I. Nonpublic Treatment

This posting contains sensitive information regarding the manner in which an entity has implemented controls to address security risks and comply with the CIP standards. As discussed below, this information, if released publicly, would jeopardize the security of the Bulk Power System and could be useful to a person planning an attack on Critical Electric Infrastructure. NERC requests that the redacted portions of this posting be designated as nonpublic under Section 39.7(b)(4) and as CEII under Section 388.113.[1]

a. The Redacted Portions of this Posting Should Be Treated as Nonpublic Under Section 39.7(b)(4) as They Contain Information that Would Jeopardize the Security of the Bulk Power System if Publicly Disclosed

Section 39.7(b)(4) of the Commission's regulations states:

> The disposition of each violation or alleged violation that relates to a Cybersecurity Incident or that would jeopardize the security of the Bulk Power System if publicly disclosed shall be nonpublic unless the Commission directs otherwise.

Consistent with its past practice, NERC is redacting information from these Compliance Exceptions, FFTs, and SNOPs according to Section 39.7(b)(4) because they contain information that would jeopardize the security of the BPS if publicly disclosed. The redacted information includes the identity of the entities and details that could lead to the identity of the entities, and information about the security of the entities' systems and operations, such as specific processes, configurations, or tools the entities use to manage their cyber systems. As the Commission has previously recognized, information related to CIP noncompliance and cyber security issues, including the identity of the registered entity, may jeopardize BPS security, asserting that "even publicly identifying which entity has a system vulnerable to a 'cyber attack' could jeopardize

[1] 18 C.F.R. § 388.113(e)(1).

system security, allowing persons seeking to do harm to focus on a particular entity in the Bulk-Power System."[2]

Consistent with the Commission's statement, NERC is treating as nonpublic the identity of the entities and any information that could lead to the identification of the entities.[3] Information that could lead to the identification of the entities includes the names, NERC Compliance Registry IDs, and information regarding the size and characteristics of the entities' operations. Entities providing electricity to the people of the United States are subject to constant attacks by malicious parties, including some supported by foreign governments. Identifying the entities in this case would highlight entities whose implementation of the CIP standards was inadequate and may be more vulnerable to cyber attacks.

NERC is also treating as nonpublic any information about the security of the entities' systems and operations.[4] Details about an entity's systems, including specific configurations or the tools/programs it uses to configure, secure, and manage changes to its BES Cyber Systems, would provide an adversary relevant information that could be used to perpetrate an attack on the entity and similar entities that use the same systems, products, or vendors.

Malicious individuals already target the entities' operational personnel, seeking bits and pieces of data to map the entities' systems and identify possible attack vectors. The public disclosure of a single piece of redacted information may not, on its own, provide everything needed to exploit an entity and attack the electric grid. But, successive public disclosures of additional pieces of redacted information will increase the likelihood of a cyber-intrusion with a corresponding adverse effect on energy infrastructure. Each successive disclosure could fill in some knowledge gaps of those planning to do harm, helping to complete the maps of entity systems. Therefore, it is important to examine and evaluate the redacted information in the aggregate.

b. <u>The Redacted Portions of this Posting Should Also be Treated as CEII as the Information Could be Useful to a Person Planning an Attack on Critical Electric Infrastructure</u>

In addition to the provisions of Section 39.7(b)(4), the redacted information also separately qualifies for treatment as CEII under Section 388.113 of the Commission's regulations. CEII is defined, in relevant part, as 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; and (2) could be useful to a person planning an attack on critical infrastructure. As discussed above, this posting includes vulnerability and design information that could be useful to a person planning an attack on the entities' critical infrastructure. The incapacity or destruction of the entities' systems and assets would negatively affect national security, economic security, and public health and safety. For example, the information includes the identification of specific cyber security issues and

---

[2] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards*, Order No. 672, 2006-2007 FERC Stats. & Regs., Regs. Preambles ¶ 31,204 at P 538 (*Order No. 672).*

[3] *See* the next section for a list of this information.

[4] *See* the accompanying document for a list of this information.

vulnerabilities, as well as details concerning the types and configurations of the entities' systems and assets. The information also describes strategies, techniques, technologies, and solutions used to resolve specific cyber security issues. Further, redacting the NERC Violation ID from the compliance history discussion ensures that an adversary will not be able to take information from multiple instances of noncompliance and aggregate that information to gain a better understanding of the entities' systems, processes, and active security measures.

The following information has been redacted from these Compliance Exceptions, FFTs, and SNOPs as CEII as the information, when viewed collectively, could be useful to a person planning an attack:

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

2. The names of the entities' vendors and contractors.

3. The names and NERC Compliance Registry numbers of the registered entities.

4. The registered functions and registration dates of the registered entities.

5. The names of registered entity facilities.

6. The names of registered entity assets.

7. The names of registered entity employees.

8. The names of departments that are unique to the registered entity.

9. The sizes and scopes of the registered entities' operations.

10. The dates of Compliance Audits of the registered entities, 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.

Under Section 388.113, NERC requests that the CEII designation apply to the redacted information in Category 1 for three years from the posting date of that document. Details about the entities' operations, networks, and security should be treated and evaluated separately from the identity to avoid unnecessary disclosure of CEII that could pose a risk to security.

The timing requests for CEII designation for Categories 2 – 12 are stated in the filing document based on the following considerations. NERC requests that the CEII designation apply to the redacted information from Categories 2 – 12 for two years from the filing date of that document for already mitigated noncompliance. For noncompliance where mitigation is not complete, NERC requests that the CEII designation apply for three years to allow for several activities that should reduce the risk to the security of the BPS. Those activities include, among others:

1. Completion of mitigation of the noncompliance;

2. Compliance monitoring of the entities to ensure sustainability of the improvements described in these noncompliance; and

3. Remediation of any subsequent noncompliance discovered through compliance monitoring by a Compliance Enforcement Authority or the entities' self-monitoring.