Critical Energy/Electric Infrastructure Information Protection Requirements

Proposal for Inclusion in a NYISO Manual

The requirements below apply to developers of generation or transmission facilities, their consultants, and any other non-governmental entities (referred to herein as "Recipients") requesting Critical Energy/Electric Infrastructure Information ("CEII") from NYISO or the New York Transmission Owners.[1] Recipients must attest to their compliance with these requirements as a condition of eligibility to receive such CEII. For the avoidance of doubt, these requirements shall only apply to CEII received from NYISO or New York Transmission Owners.

For purposes of these Requirements, CEII is defined according to the Federal Energy Regulatory Commission ("FERC") regulations, 18 C.F.R. § 388.113(c):

> **Critical Electric Infrastructure Information** means information related to critical electric infrastructure, or proposed critical electrical infrastructure, generated by or provided to the FERC 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. Such term includes information that qualifies as critical energy infrastructure information under the Commission's regulations. Critical Electric Infrastructure Information is exempt from mandatory disclosure 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 section 215A(d)(1)(A) and (B) of the Federal Power Act.
>
> **Critical Energy Infrastructure Information** means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:
> - Relates details about the production, generation, transportation, transmission, or distribution of energy;
> - Could be useful to a person in planning an attack on critical infrastructure;
> - Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
> - Does not simply give the general location of the critical infrastructure.
>
> **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.

[1] The New York Transmission Owners include: Central Hudson Gas & Electric Corporation ("Central Hudson"), Consolidated Edison Company of New York, Inc. ("Consolidated Edison"), Niagara Mohawk Power Corporation d/b/a National Grid ("National Grid"), New York Power Authority ("NYPA"), New York State Electric & Gas Corporation ("NYSEG"), Orange and Rockland Utilities, Inc. ("O&R"), Long Island Power Authority ("LIPA"), and Rochester Gas and Electric Corporation ("RG&E").

Critical infrastructure means existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters.

Company Information and Insurance Requirements

1. Recipient shall provide to NYISO and the Transmission Owner, if applicable, a list of any countries other than the United States or Canada in which Recipient operates (has an office, sells product, or conducts any business) and a description of activities conducted in each.

2. Recipient shall maintain cyber security risk insurance in coverage amounts of $5 million.

Supply Chain and External Dependencies Management

Recipient shall:

1. Have policies to confirm that all agreements or contracts with Recipient's service provider(s) contain specific clauses to protect data or systems used to store CEII when those systems are accessed, processed, or stored by its third-party suppliers/service providers.

2. Have an established program that provides for storage security of CEII at Recipient's site (*e.g.*, chain of custody).

3. Have a process to confirm the source of software downloads and the integrity of the software downloaded prior to use in Recipient's computer and information systems used for handling CEII.

4. Have a process to verify that procured products used for handling CEII (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to being placed in production.

5. Have an information protection program that includes safeguards and notifications regarding the release of CEII data to third parties. Evidence of such safeguards and notifications could include, but is not limited to:
    a. records of third party entities and the CEII data that they have access to; and
    b. a description of why each of these parties requires access to such CEII data.

Recipient is itself not a person subject to subparagraphs (1), (2), or (3) below; and Recipient has not engaged and will not engage in any transaction that could put CEII at risk with an entity:

1. owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary," as defined by 15 C.F.R. § 7.2 or by the Department of Energy in any order or regulation;

2. with whom transactions are prohibited by regulations promulgated under the International Emergency Economic Powers Act or any other state or federal law;

3. listed on the International Trade Administration's Consolidated Screening List or identified as excluded on the General Services Administration's System for Award Management; or

4. otherwise identified by NYISO as posing a security risk.

Workforce Management

Recipient shall have a process or procedure to:

1. Perform background screenings for personnel accessing CEII, including employees, contractors, and subcontractors.

2. Provide mandatory security awareness training, including CEII training, at least annually.

Identity and Access Management

Recipient shall:

1. Establish and maintain an identity and access management program, including the following:

    a. Emphasize password/passphrase complexity and aging requirements or equivalent controls for computing systems used to store CEII.

    b. Provide for computing systems used to store CEII that have user account passwords/passphrases that are stored must be encrypted at rest.

    c. Has a process or policy to develop and maintain audit logs for computing systems used to store CEII that include at least all of the following: login, logout, actions performed, and the source IP address.

    d. Have a process or policy for administering administrative accounts on systems used to store CEII.

2. Have a process or procedure to deploy and maintain hardware authentication devices and/or maintain computing system applications that support multi-factor authentication (*e.g.*, Duo, Google Authenticator, OTP, etc.) for interactive remote access to any system that stores CEII and ensure that such multi-factor authentication systems are mandatory for all personnel.

Cybersecurity Program Management

1. Recipient's information protection program shall provide for secure deletion (*e.g.*, degaussing/cryptographic wiping) or destruction of CEII, including archived or backed-up data.

2. Recipient shall have and follow documented operating procedures and technological controls to provide for effective management, operation, integrity, and security of information systems and data used to store CEII.

Change and Configuration Management

1. Recipient shall adhere to a documented change management process ("CMP") for assets under its control that store CEII, including among other things to assess and deploy vendor security patches in a reasonable time frame on assets used to store CEII.

Data Protection

1. Recipient's information protection program shall:

    a. Include managing and securing data at rest and in transit to ensure confidentiality, integrity, and availability (*e.g.*, implement encryption or technology to restrict access and obfuscate sensitive data).

    b. Address all technologies in use (*e.g.*, on-premise, co-located, off-site, cloud, etc.).

2. Recipient shall have a documented program to identify, classify, protect, manage, and maintain CEII information.

3. Recipient's workstations and mobile devices used to store CEII shall be encrypted.

Event and Incident Response

1. Recipient shall have a cyber security incident response plan/process, including a process to provide prompt notification to the NYISO and to the applicable New York Transmission Owner, within 48 hours , upon the Recipient discovering that a cyber security incident[2] of the system containing CEII and has affected the security of CEII data.

2. Recipient shall review and update its cyber security incident response plan at least annually.

Risk and Vulnerability Management

1. Recipient shall have up-to-date antivirus on its computer and information systems used to store CEII.

[2] Cyber security incident shall mean the same meaning as defined by NERC ("a malicious act or suspicious event of a system that compromises or an attempt to compromise").

2. Recipient shall have a risk management policy, procedure, and program that provides for the physical security of CEII.