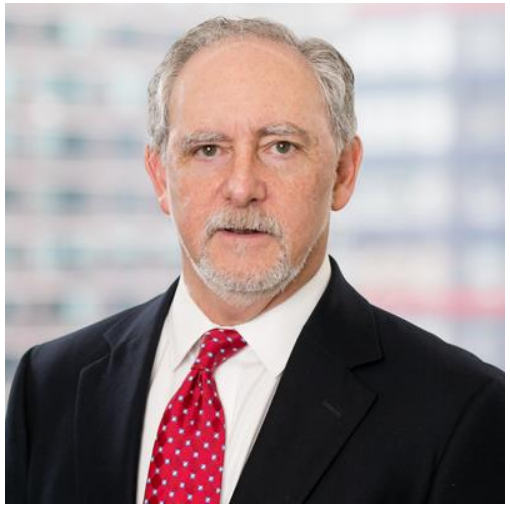
# NYISO Critical Energy/Electric Infrastructure Information (CEII) Protection Requirements

September 21, 2023

troutman pepper

# Presenters




## Stu Caplan

Partner

stuart.caplan@troutman.com

212.704.6060



## Kat O’Konski

Associate

katherine.okonski@troutman.com

202.274.2803

# Agenda

## Background – Regulatory Landscape

- NERC CIP Requirements
- Critical Energy/Electric Infrastructure Information (CEII) Definitions
- FERC CEII Protection and Sharing Rules
- NYISO's CEII Protection and Sharing Rules

## Current CEII Requirements Do Not Adhere to Industry Standards

## Proposed Improvements

- CEII Requirements (NYISO Manual)
- Attestation
- Tariff Language

# Background – Regulatory Landscape

- **NERC Critical Infrastructure Protection (CIP) Reliability Standards**
- Provide a comprehensive set of requirements to protect the bulk power system from malicious attacks.
- Consist of 11 standards and over 45 requirements covering the security of electronic perimeters and the protection of critical cyber assets as well as personnel and training, security management and disaster recovery planning.
- Addresses supply chain risk management and information protection requirements, among other priorities.
- CIP standards apply to NERC-registered entities.

# Background – Regulatory Landscape

## CEII Definitions - 18 C.F.R. § 388.113

| Key Terms | |
|---|---|
| Critical **Electric** Infrastructure Information<br><br>§ 388.113(c)(1),(3) | • Information related to critical electric infrastructure, generated or provided to FERC or other federal agencies<br>• Designated as CEII by FERC or Secretary of Energy<br>• Exempt from mandatory disclosure under FOIA<br><br>Critical Electric Infrastructure: 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. |
| Critical **Energy** Infrastructure Information<br><br>§ 388.113(c)(2) | any specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:<br>•Relates details about the production, generation, transportation, transmission or distribution of energy;<br>•Could be useful in planning an attack on critical energy infrastructure;<br>•Is exempt from mandatory disclosure under FOIA; and<br>•Provides information beyond general location of critical energy infrastructure. |



troutman pepper

# Background – Regulatory Landscape

- **FERC CEII Protection Rules**
- Apply only to information submitted to or generated by FERC.  Protections do not apply to information exchanged at the ISO level.
- FERC employees and contractors have a duty to protect CEII from unauthorized disclosure and may be subject to sanctions for knowing/willful unauthorized disclosure.  18 C.F.R.§ 388.113(h).
- Access Rules - 18 C.F.R.§ 388.113(g):
  - Owners/operators of facilities may obtain CEII relating to their own facilities, excluding certain FERC-generated information, via request to FERC's CEII Coordinator.
  - Employees of federal agencies acting within the scope of their employment may access CEII (must execute an agreement to protect in the same manner as FERC).
  - Landowners whose properties are crossed by or in the vicinity of a project may access certain CEII without submitting an NDA.
  - For CEII submitted to FERC in FERC proceedings: Intervenors may make a written request to the filer for CEII, along with an executed version of the applicable protective agreement.
  - Others may request access from FERC's CEII Coordinator (requires detailed statement of need and executed NDA).



troutman pepper

# Background – Regulatory Landscape

- **FERC's CEII Non-Disclosure Agreement (NDA)** (developed in 2016):
  - CEII may only be discussed with another authorized recipient of identical CEII.
  - Only used for the purpose for which it was requested.
  - Can be used as foundation for advice provided to others, but not shared.
  - Copies permitted but must be marked CEII.
  - Must be maintained in secure manner to prevent unauthorized access.
  - Must be destroyed or returned to FERC within 15 days of a written request.
  - CEII must be protected as long as it is in a recipient's possession, unless the CEII Coordinator determines the information should no longer be designated as CEII.
  - Unauthorized disclosure reported to FERC; FERC may audit recipient's compliance.
  - Improper handling (violation of the NDA) may result in criminal or civil sanctions.



troutman pepper

# Background – Regulatory Landscape

- **NYISO CEII Protection Rules**
- Requestors must sign NYISO's CEII NDA: https://nyiso.tfaforms.net/187
  - CEII must be stored securely.
  - Copies permitted but become subject to the NDA.
  - CEII may only be used for the purpose specified by the recipient in NYISO's request form.
  - CEII must be returned to NYISO upon request; NDA remains in effect until the information is returned to NYISO (or information is no longer classified as CEII).
- CEII requests are specific to an individual.
- Requestors must create a MyNYISO account.



troutman pepper

# Current CEII Protections Do Not Adhere to Industry Standards

- NYISO NDA requires information to be stored “securely” but contains no cybersecurity requirements to ensure that information is secure.
  - Current NYISO requirements lack basic, industry-standard requirements to protect information, e.g.:
    - Multi-factor authentication.
    - Encryption requirements for handling/exchanging CEII.
    - Deletion/destruction requirements when CEII is no longer needed.
    - Security incident notification requirements.
- NYISO’s NDA applies on an individual, rather than organizational, level.

# Recent Events Underscore the Importance of Robust Cybersecurity Measures

- Risk associated with loss or unauthorized disclosure is significant.
- Changing Threat Landscape:
  - 2020 SolarWinds cyberattack impacted some utilities and the DOE.
  - 2021 Colonial Pipeline attack.
  - 2022 Sargent & Lundy ransomware attack; models, transmission data compromised.
  - 2023 MOVEit global cyberattack on widely-used data transfer software impacted US government agencies including the DOE; several hundred companies.
  - Physical attacks and vandalism at electric utility substations.



troutman pepper

# Proposal to Improve Security of CEII at the NYISO level

1. New CEII protection requirements described in a NYISO Manual (CEII Requirements).
2. All CEII requestors attest to compliance with CEII Requirements.
3. New Tariff language to require CEII requestors to sign attestation of compliance with the CEII Requirements.



troutman pepper

# Proposed CEII Protection Requirements

**New requirements proposed for inclusion in a NYISO manual, based on North American Transmission Forum (NATF) questionnaire, a NERC-approved tool.**

- Supply Chain requirements:
  - Agreements with contractors must address data protection.
  - Program to ensure security of data stored with recipient.
  - Requirements to log release of data to third parties.
- Workforce management requirements:
  - Background check requirements.
  - Mandatory security awareness and privacy training for employees.

# Proposed CEII Protection Requirements, Continued

- Access Management Requirements:
  - Tracking of individuals' access to sensitive information.
  - Password complexity and aging requirements.
  - Multi-factor authentication requirement.
- Cybersecurity Program Requirement
- Data Protection Requirements:
  - Encryption requirements.
  - Geographic requirements for storage (US and Canada).
  - Data destruction requirements.

# Proposed CEII Protection Requirements, Continued

- Incident Response Requirements:
  - Process to notify NYISO and Transmission Owner (if applicable) within 24 hours of a cyber or physical security incident that could affect the security of CEII.
- Risk and Vulnerability Management:
  - Updated anti-virus and other security controls.
  - Risk management policies and procedures.
  - Vulnerability assessment requirements.

# Attestation and Tariff Language

- Additional steps to ensure compliance:
  - Sector-wide attestation requirement ensures NYISO is able to administer the program.
  - Attestation to be signed at an organizational level.
  - NYISO's existing NDA would continue to apply at an individual level.
- NYISO tariff language to require compliance with CEII requirements and for all CEII requestors to execute the attestation.
  - Proposed CEII requirements would have sector-wide applicability. As a result, broadly-applicable tariff provisions would be required.



troutman pepper

# Next Steps

- The NYTOs request stakeholder review and comment on this proposal by **September 28, 2023**.
  - Direct comments to:
    - **Stu Caplan**: stuart.caplan@troutman.com
    - **Kat O'Konski**: katherine.okonski@troutman.com
- The NYTOs will consider stakeholder comments and plan to return to stakeholders with a more detailed proposal.



troutman pepper

# Questions?