Date Filed: November 16, 2026

Witness: Christopher E. Colorio, Leanne M. Landry and Jeffrey D. Turano
Request from: Public Utilities Regulatory Authority

Question:

(Plant Additions) Application, CLP-Additions-4. Regarding Project Nos. CD21730 and CTDSOCIT related to the Windsor System Operations Center, state whether the projects are in compliance with NERC CIP requirements. If so provide:

a. The specific NERC CIP requirements with which the projects comply;

b. The reasons justifying the need to comply NERC CIP requirements; and

c. A list of all distribution plant additions by item category (e.g., physical security, SCADA changes) for each project that was done to ensure compliance with NERC CIP requirements.

Response:

For large projects, Reliability Compliance develops a "CIP Compliance Plan" for purposes of documenting the impacted CIP Standards. Reliability Compliance worked with the project team to identify scope and applicable CIP Standards. The project scope involved the relocation of the CT System Operation Center (SOC) from Berlin, CT to Windsor, CT with planned in-service date in Q1 2026. The list of applicable CIP Standards for this project are identified below:

Standard	Business Owner(s)	Approach	Justification to comply with CIP Standard
CIP-002	IT Real-Time Systems / Asset Management	Document New Bulk Electric System (BES) Cyber Assets (BCA): • Identify, classify, and map all new BCSs and BCAs. • Update BCS List (Critical Assets List) before cut-over. • Declassify after parallel operation.	Addition of new BCA's requires identification and classification per CIP-002.
CIP-003	IT Security NERC CIP Senior Manager	New CIP Sites Activated & Operational: • Create CIP Design plan to ensure all CIP Requirements are met before activating the new BCAs and BCSs. • Obtain CIP Senior Manager approval of CIP Design plan.	CIP Senior Manager to sign-off on CIP Compliance Plan prior to go-live.
CIP-004	Corporate Security	Access to the new PSP Management in Place: • Identify all personnel requiring access to the new BCAs and BCSs. Provision access to the new PSP where appropriate. • Remove users not needing access post cut-over.	CIP physical access provisioning required at new SOC location.
CIP-005	IT Security / IT Real-Time Systems	Document & Activate New Electronic Security (ESP): • Identify network locations of all new BCAs and BCSs to be electronically protected before activation. Update network diagrams as needed. • Update CIP-005 4Ps, as necessary.	New ESP established and network drawings updated

Standard	Business Owner(s)	Approach	Justification to comply with CIP Standard
CIP-006	Corporate Security	Document & Activate New Physical Security (PSP): • Identify all newly required PSPs locations and the necessary security measures to be added were communicated to the project team.	All physical security measures (card access panels, cameras, etc.) installed at new SOC location
CIP-007	IT Security / IT Real-Time Systems	Document & Activate New System Security Controls: • Put in place CIP Security measures using appropriate security tools. • Identify all newly required ESP modifications and the necessary security measures to be added. • Inventory of all accounts and passwords is completed and up to date. • Reset passwords before cut-over or enter in CyberArk.	Implement system security controls at new SOC location including documenting ports & services, deployment of malicious code prevention, deployment of security event monitoring and document generic/shared ID accounts that support system access control.
CIP-008	IT Security	Update & Activate System Incident Reporting & Recovery: • Notify the owner(s) to update Incident Reporting and Recovery plan.	Update Incident Reporting and Recovery Plan to reflect any changes in roles and responsibilities.
CIP-009	IT Real-Time Systems	Update & Activate Cyber System Recovery Plan: • Notify Cyber System Recovery Plan owners to apply needed updates to the Cyber System Recovery plans. • CIP-009-PRO-01 to 13 – SMEs to review and coordinate updates.	Update CIP recovery plans where applicable.

Standard	Business Owner(s)	Approach	Justification to comply with CIP Standard
CIP-010	IT Security / IT Real-Time Systems	Update & Activate Configuration Change Management Plan: • Identify Configuration change owners so that they are prepared to follow company procedures. • Implement New CIP Protected Asset Procedure in CIP-010-PRO-05, Appendix A. • Perform an active vulnerability assessment of all the new Cyber Assets	Onboard new BCA's and follow change management process. Conduct an active vulnerability assessment on new BCA's.
CIP-011	IT Real-Time Systems	Update & Activate Information Protection Plan: • Documentation will be stored in CIP folders as per Eversource Information Protection standards. • Implement Eversource process to dispose of existing Berlin SOC assets (documentation / physical assets)	Ensure CIP protected information is identified, stored and labeled consistent with Eversource CIP procedures
CIP-012	IT Security / IT Real-Time Systems	Communications between Control Centers Plan: • Update CIP-012-PLN-01	Update control center communications between Local Control Center and Windsor SOC.
CIP-013	IT Security / IT Real-Time Systems	Supply Chain Cyber Security Risk Management Plan: • Document a list of vendors and their CIP-013 compliance status in a CIP folder. • Ensure a fully executed CIP-013 CIP Compliance Agreement (CCA) is on file at Procurement.	Ensure vendors go through risk assessments and execute CCA

To ensure compliance with all CIP standards associated with this project, the project team assigned 'Business Owners' to these Standards. The 'Business Owners' were responsible for ensuring the "CIP Compliance Plan" is successfully executed and we maintain compliance during relocation.