Summary of Proposed Reliability Standard: Project 2019-02 BES Cyber System Information Access Management

Reliability Standards Authority: **NERC**

Standards/Purpose: CIP-004-7 — Cyber Security – Personnel & Training

CIP-011-3 — Cyber Security — Information Protection

Change Type: FERC Directive

Affected Functional Entities: Balancing Authority (BA)

Distribution Provider (DP)

Generator Operator (GOP)

Generator Owner (GO)

Reliability Coordinator (RC)

Transmission Operator (TOP)

Transmission Owner (TO)

Non-Ansi Standard: No

Ballot Results: CIP-004-7 86.5% Quorum/ 85.8% Approval
CIP-011-386.5% Quorum / 83.0% Approval

Technical Impact in Ontario: None

Costs of Implementation: None

Ontario Participant Support: Ontario voted supported the proposed changes.

Reliability Standard Milestones:

Date	Action
	Adopted by NERC Board of Trustees
September 15, 2021	NERC Petition for Approval
September 21, 2021	IESO Posting Date
January 19, 2022	End of OEB Review Period
TBD	FERC Order Issued
TBD	US Mandatory Enforcement Date
TBD	Ontario Enforcement Date (Milestones in Reliability Standard Development and Lifecycle)

ieso
Independent Electricity System Operator

Summary:

The suite of Critical Infrastructure Protection ("CIP") Reliability Standards require protections around BES Cyber Systems, the most critical cyber devices on the electric grid. As defined in the NERC Glossary of Terms used in Reliability Standards ("NERC Glossary"), BCSI is "information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System." Given the importance of BCSI, Responsible Entities must control access to this information. In currently effective Reliability Standards CIP-004-6 and CIP-011-2, Responsible Entities do this by managing access to the "designated storage location" of BCSI, such as an electronic document or physical file room. However, as technology has evolved, third-party services, such as cloud services, have become a viable and safe option for storing BCSI. The protections available for Responsible Entities to secure information in the cloud, for example, depend less on the actual storage location of the information and more on file-level rights and permissions. As a result, the revisions in proposed Reliability Standards CIP-004-7 and CIP-011-3 would allow Responsible Entities to leverage these protections within their control for third-party data storage and analysis systems. To that end, proposed CIP-004-7, which pertains to personnel and training, includes the following modifications:

- Removes references to "designated storage locations" of BCSI;
- Adds Requirement R6 regarding an access management program to authorize, verify, and revoke provisioned access to BCSI; and
- Other minor clarifications to update the standard.

Proposed Reliability Standard CIP-011-3, which pertains to information protection, includes the following modifications:

- Clarifies requirements regarding protecting and securely handling BCSI; and
- Other minor clarifications to update the standard.

The proposed Reliability Standards maintain the security objectives supported in previous versions while providing flexibility for Responsible Entities to leverage third-party data storage and analysis systems.

Other Salient Information

None.