Summary NERC Project 2019-03 Cyber Security Supply Chain Risks Management

Reliability Standards Authority:	NERC
Standards:	CIP-005-6 - Cyber Security - Electronic Security Perimeter(s) CIP-010-3 - Cyber Security - Configuration Change Management and Vulnerability Assessments CIP-013-1 - Cyber Security - Supply Chain Risk Management
Purpose	The purpose of this project is to address the directives issued by FERC in Order No. 850 and address NERC staff recommendation from the Supply Chain Report.
Change Type:	FERC Directive
Affected Functional Entities:	Balancing Authority (BA), Distribution Provider (DP), Generator Owner (GO), Generator Operator (GOP), Reliability Coordinator (RC), Transmission Operator (TOP), Transmission Owner (TO),
Non-Ansi Standard:	No
Ballot Results:	Quorum: 85.56% Approval 76.76%-
Costs of Implementation:	Not Assessed
Ontario Participant Support:	The Standard Drafting Team included representation from Ontario

Reliability Standard Milestones:

Date	Action
	Adopted by NERC Board of Trustees
December 21, 2020	NERC Petition for Approval
December 29, 2020	IESO Posting Date
April 28, 2021	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)

Summary:

This project aligns NERC Standards with the NERC Supply Chain Report, and addressed the directives issued by FERC in Order No. 850 to modify the Supply Chain Standards. FERC directed NERC to submit modifications to address Electronic Access Control or Monitoring Systems (EACMSs) specifically those systems that provide electronic access control to high and medium impact BES Cyber Systems. Proposed Reliability Standards CIP-013-2, CIP-005-7, and CIP-010-4 (proposed "Supply Chain Standards") broaden supply chain risk management requirements to include EACMS and PACS as applicable systems.

EACMS are devices that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter ("ESP") or BES Cyber Systems. As such, EACMS (e.g., firewalls or security information event management systems, among others) control or monitor electronic access to some of the most critical systems operating the BES. PACS are devices that control alert, or log access to the Physical Security Perimeter ("PSP"). These devices help to manage physical access to defined areas that physically contain medium and high impact BES Cyber Systems. Similar to EACMS, PACS manage physical access to some of the most critical systems operating the BES. As such, including both EACMS and PACS as applicable systems in the Supply Chain Standards further enhances the reliability of the BES. The proposed Reliability Standards maintain the security objectives supported in the original version of the Supply Chain Standards while expanding protections for these additional applicable systems.

Other Salient Information

No technical and financial impacts have been assessed