NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005-7 Summary of Changes

Project 2019-03 Cyber Security Supply Chain Risks

In an effort to assist industry during the second posting of Project 2019-03, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-005-7. The SDT is proposing language in CIP-005-7 in the newly formed R3 to include EACMS as an applicable system to address industry concern during the initial ballot concerning the required use of Intermediate Systems and EACMS. This proposed requirement has modified language from CIP-005-6 Requirement R2.4 and R2.5 and is not a wholly new requirement from the previous version of the standard. The comparison below shows the modifications from CIP-005-6 Requirement 2 Part 2.4 and Part 2.5 to CIP-005-7 Requirement 3 Part 3.1 and Part 3.2.

CIP-005-6 Language	CIP-005-7 Language
Requirement R2, Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.1: Have one or more methods for ~~determining~~ detecting ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.
Requirement R2, Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Requirement R3, Part 3.2: Have one or more method(s) to ~~disable~~ terminate established ~~active~~ vendor-initiated remote access sessions ~~(including Interactive Remote Access and system-to-system remote access)~~.