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 third posting of Project 2019-03, the Standard Drafting Team (SDT) has prepared the summary of changes document for CIP-005-7.

To address industry concern during the second ballot regarding the required use of Intermediate Systems and EACMS, and the creation of a 'hall of mirrors', the SDT is proposing to restore CIP-005-7 Requirement R2 Parts 2.4 and 2.5 to the original approved CIP-005-6 language and Applicable Systems.

To further address this concern, the SDT is proposing the newly formed Requirement R3 be dedicated to addressing vendor remote access for EACMS and PACS, specifically. To further address industry concern, references to Interactive Remote Access (IRA) and the undefined term system to system were removed.

The first table shows the current approved CIP-005-6 as compared to the current posting of CIP-005-7.

Current approved CIP-005-6 Language	**CIP-005-7 Language – Current Posting**
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 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 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 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: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS.* [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
	Requirement R3, Part 3.1: Have one or more method(s) to determine authenticated vendor-initiated remote connections.
	Requirement R3, Part 3.2: Have one or more method(s) to terminate authenticated vendor-initiated remote connections sessions and control the ability to reconnect.

This second table shows the last posted draft as compared to the current posting of CIP-005-7.

This illustrates Requirement R2, Part 2.4 and Part 2.5, which had been moved to R3 in the last posting, are back in R2 restoring CIP-005-6 and its Applicable Systems to the current approved language: High impact BES Cyber Systems and their associated to PCAs, and Medium impact BES Cyber Systems with External Routable Connectivity and their associated to PCAs.

This also demonstrates Requirement R3 has been modified to focus solely on EACMS and PACS associated to high impact BES Cyber Systems, and EACMS and PACS associated to medium impact BES Cyber Systems with External Routable Connectivity. The language of Requirement R3, Part 3.1 and Part 3.2 have been modified to 1) remove 'access' to address double jeopardy concerns with CIP-004-6; 2) replace 'detecting' with 'authenticate' to address concerns about real-time monitoring of vendor activity; and 3) replace 'sessions' with 'connections' to address industry concerns about ambiguity with the term 'session'.

CIP-005-7 Language – Last Posted second draft	**CIP-005-7 Language – redline from Last Posted**
	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 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: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*	Requirement R3: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS*. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].
Requirement R3, Part 3.1: Have one or more methods for detecting vendor-initiated remote access sessions.	Requirement R3, Part 3.1: Have one or more methods to determine authenticated ~~for detecting~~ vendor-initiated remote connections~~access sessions~~.
Requirement R3, Part 3.2: Have one or more method(s) to terminate established vendor-initiated remote access sessions.	Requirement R3, Part 3.2: Have one or more method(s) to terminate authenticated~~established~~ vendor-initiated remote connections~~access sessions~~ and control the ability to reconnect.