NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# CIP-013-2 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-013-2.

To address the FERC directives, EACMS and PACS were added to Requirements R1 and R2.

The first table shows the current approved CIP-013-1 as compared to the current posting of CIP-013-2.

| Current approved CIP-013-1 Language | CIP-013-2 Language – Current Posting |
|---|---|
| **Requirement R1:**<br>Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* | **Requirement R1:**<br>Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated EACMS and PACS. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]* |
| **Requirement R1.1:**<br>One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s). | **Requirement R1.1:**<br>One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s). |
| **Requirement R1.2:**<br>One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable: | **Requirement R1.2:**<br>One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable: |
| **Requirement R1.2.5:**<br>Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and | **Requirement R1.2.5:**<br>Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and |
| **Requirement R1.2.6:**<br>Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s). | **Requirement R1.2.6:**<br>Coordination of controls for (i) vendor-initiated ~~Interactive R~~remote ~~A~~access~~, and (ii) system to system remote access with a vendor(s)~~. |

This second table shows the last posted draft as compared to the current posting of CIP-013-2.

To address industry concern during the second ballot regarding 'hall of mirrors' for EACMS and the required use of Intermediate Systems, as well as concerns about inconsistencies in language between procurement planning requirements in CIP-013-2 and the operational security requirements of CIP-005-7, references to Interactive Remote Access (IRA) and the undefined term system to system were removed from, CIP-013-2 Requirement R1.2.6, because authenticated remote connections and system to system remote connections for EACMS and PACS; and IRA and system to system access to BCS and PCAs are all sub-types of vendor-initiated remote access.

| CIP-013-1 Language – Last Posted second draft | CIP-013-2 Language – Current Posting |
|---|---|
| **Requirement R1.2.6:**<br>Coordination of controls for (i) vendor-initiated remote access, and (ii) system-to-system remote access with a vendor(s). | **Requirement R1.2.6:**<br>Coordination of controls for ~~(i)~~ vendor-initiated remote access~~, and (ii) system-to-system remote access with a vendor(s)~~. |