

## Consideration of Issues and Directives

### Project 2019-03 Cyber Security Supply Chain Risks

Project 2019-03 Cyber Security Supply Chain Risks		
Issue or Directive	Source	Consideration of Issue or Directive
Develop modifications to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the supply chain risk management Reliability Standards.	FERC Order No. 850, P 5 and P 30	<p>The SDT proposed the modified language in CIP-005-7 Requirement R3 and CIP-010-4 Requirement R1.6 to include EACMS as an applicable system <u>for supply chain requirements</u>. <del>These requirements are the supply chain requirements embedded in the CIP-005 and CIP-010 requirements.</del> Proposed CIP-005-7 Requirement R3 is a new requirement that includes <u>methods to determine and terminate authenticated vendor-initiated remote connections for EACMS, which is similar to requirements Parts 3.1 and 3.2 in CIP-005-7 were previously located in Parts 2.4 and 2.5 for other applicable systems. in CIP-005-6, and include modifications from the language used in CIP-005-6.</u></p> <p>Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include EACMS per the FERC directive.</p>
Develop modifications to include PACS associated with medium and high impact BES Cyber Systems within the	NERC – Cyber Security Supply Chain	<p>The SDT proposed the modified language in CIP-005-7 Requirement R3 and CIP-010-4 Requirement R1.6 to include PACS as an applicable system <u>for supply chain requirements</u>. <del>These requirements are the supply chain requirements</del></p>

**Project 2019-03 Cyber Security Supply Chain Risks**

Issue or Directive	Source	Consideration of Issue or Directive
<p>scope of the supply chain risk management Reliability Standards.</p>	<p>Risks, Chapter 2</p>	<p><del>embedded in the CIP-005 and CIP-010 requirements.</del> Proposed <u>CIP-005-7 Requirement R3 is a new requirement that requires processes that include methods to determine and terminate authenticated vendor-initiated remote connections for PACS, which is similar to requirements Parts 3.1 and 3.2 in CIP-005-7</u> <del>were previously located</del> in Parts 2.4 and 2.5 <u>for other applicable systems. in CIP-005-6, and include modifications from the language used in CIP-005-6.</u></p> <p>Standard CIP-013-2 deals with Cyber Security – Supply Chain Risk Management. Requirement R1 was modified to include PACS per the FERC directive.</p>