Order No. 829 Citation	Directive / Guidance	Resolution
P 43	[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.	Proposed CIP-013-1 addresses the directive. The purpose of the proposed standard is: *To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.* The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations". High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the

Order No. 829 Citation	Directive / Guidance	Resolution
		development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.
P 44	[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. NERC should submit an informational filing [by December 26, 2016] with a plan to address the Commission's directive.	The proposed/modified standard(s) must be filed by September 27, 2017. NERC filed its plan to address the directive on December 15, 2016.
P 45	The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve	The directive is addressed by Requirements R1, R2, and R3 of proposed CIP-013-1. Requirement R1 specifies that entities must develop, and Requirement R2 specifies that entities must implement, one or more documented supply chain cyber security risk

Order No. 829 Citation	Directive / Guidance	Resolution
	these four objectives but have the flexibility as to how to reach the objective (i.e., the Reliability Standard should set goals (the "what"), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how")).	management plan(s) for high and medium impact BES Cyber Systems that include one or more process(es) for mitigating cyber security risks to BES Cyber Systems. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle. **Proposed CIP-013-1 Requirement R1** **R1.** 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: **1.1.** 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). **1.2.** One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable: **1.2.1.** Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity; **1.2.2.** Coordination of responses to vendor-identified incidents related to the products or services provided to the

Order No. 829 Citation	Directive / Guidance	Resolution
		Responsible Entity that pose cyber security risk to the Responsible Entity; **1.2.3.** Notification by vendors when remote or onsite access should no longer be granted to vendor representatives; **1.2.4.** Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity; **1.2.5.** Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and **1.2.6.** Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s). **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.
P 46	The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1, the Reliability Standard should require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months. This periodic assessment should better ensure	The directive is addressed in proposed CIP-013-1 Requirement R3. **Proposed CIP-013-1 Requirement R3** **R3.** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months

Order No. 829 Citation	Directive / Guidance	Resolution
	that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	
p 47	Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.	The directive is addressed in proposed CIP-013-1 Requirement R3 (shown above) and supporting guidance. **Proposed CIP-013-1 Rationale for Requirement R3:** Entities perform periodic assessment to keep plans up-to-date and, addressing current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC) *Implementation Guidance* developed by the drafting team and submitted for ERO endorsement includes example controls.
Objective 1: Software Integrity and Authenticity		
P 48	The new or modified Reliability Standard must address verification of: (1) the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and (2) the integrity of the software and patches before they are installed in the BES Cyber System environment.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2.5 (discussed above) and CIP-010-3 Requirements R1 Part 1.6. The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit. **Proposed CIP-010-3 Requirement R1** **R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*.

Order No. 829 Citation	Directive / Guidance	Resolution
		1.6. Prior to change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: **1.6.1.** Verify the identity of the software source; and **1.6.2.** Verify the integrity of the software obtained from the software source.
Objective 2: Vendor Remote Access to BES Cyber Systems		
P 51	The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.	The directive is addressed by proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5. The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach. **Proposed CIP-005-6 Requirement R2** **R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically

Order No. 829 Citation	Directive / Guidance	Resolution
		feasible, in CIP-005-6 Table R2 –Remote Access Management.: **2.4** Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access). **2.5** Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
P 52	In addition, controls adopted under this objective should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.	The directive is addressed by CIP-005-6 Requirement R2 Part 2.5 (above).
Objective 3: Information System Planning and Procurement		
P 56	As part of this objective, the new or modified Reliability Standard must address a responsible entity's CIP Senior Manager's (or delegate's) identification and documentation of the risks of proposed information system planning and system development actions. This objective is intended to ensure adequate consideration of these risks, as well as the available options for hardening the responsible entity's information system and minimizing the attack surface.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.1 (shown above).
Objective 4: Vendor Risk Management and Procurement Controls		
P 59	The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. Specifically, NERC must address controls for	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).

Order No. 829 Citation	Directive / Guidance	Resolution
	the following topics: (1) vendor security event notification processes; (2) vendor personnel termination notification for employees with access to remote and onsite systems; (3) product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; (4) coordinated incident response activities; and (5) other related aspects of procurement. NERC should also consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.	