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.*
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 standard 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 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")).	The directive is addressed by Requirements R1, R3, R4, and R5 of proposed CIP-013-1. Requirement R1 specifies that entities must implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle as described further below.

Order No. 829 Citation	Directive / Guidance	Resolution
		Proposed CIP-013-1 Requirement R1 **R1.** Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: **1.1.** The use of controls in BES Cyber System planning and development to: **1.1.1.** Identify and assess risk(s) during the procurement and deployment of vendor products and services; and **1.1.2.** Evaluate methods to address identified risk(s). **1.2.** The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets: **1.2.1.** Process(es) for notification of vendor security events;

Order No. 829 Citation	Directive / Guidance	Resolution
		1.2.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted; **1.2.3.** Process(es) for disclosure of known vulnerabilities; **1.2.4.** Coordination of response to vendor-related cyber security incidents; **1.2.5.** Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use; **1.2.6.** Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and **1.2.7.** Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.
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 that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	The directive is addressed in proposed CIP-013-1 Requirement R2. **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include: **2.1.** Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and

Order No. 829 Citation	Directive / Guidance	Resolution
		2.2. Obtaining CIP Senior Manager or delegate approval.
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 R2 part 2.1 (shown above) and supporting guidance. **Proposed CIP-013-1 Rationale for Requirement R2:** Order No. 829 also directs that the periodic assessment "ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities" (P. 47). Examples of sources of information that the entity considers include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC) *Technical Guidance and Examples* document developed by the drafting team 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 Requirements R3 and R5 Part 5.1. Requirement R3 applies to high and medium impact BES Cyber Systems. Requirement R5 applies to low impact BES Cyber Systems. **Proposed CIP-013-1 Requirement R3** **R3.** Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and

Order No. 829 Citation	Directive / Guidance	Resolution
		firmware before being placed in operation on high and medium impact BES Cyber Systems: **3.1.** Operating System(s); **3.2.** Firmware; **3.3.** Commercially available or open-source application software; and **3.4.** Patches, updates, and upgrades to 3.1 through 3.3. **<u>Proposed CIP-013-1 Requirement R5</u>** **R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: **5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and...
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-013-1 Requirement R4 Part 4.1 and 4.2 and Requirement R5 Part 5.2. Requirement R4 applies to high and medium impact BES Cyber Systems. Requirement R5 applies to low impact BES Cyber Systems.

Order No. 829 Citation	Directive / Guidance	Resolution
		Proposed CIP-013-1 Requirement R4 **R4.** Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): **4.1.** Authorization of remote access by the Responsible Entity; **4.2.** Logging and monitoring of remote access sessions to detect unauthorized activity; and **4.3.** Disabling or otherwise responding to unauthorized activity during remote access sessions. **Proposed CIP-013-1 Requirement R5** **R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: **5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).

Order No. 829 Citation	Directive / Guidance	Resolution
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 Requirement R4 Part 4.3 (above) and Requirement R5 Part 5.2 (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 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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).