Unofficial Comment Form

Project 2016-03 Cyber Security

Supply Chain Risk Management

**DO NOT** use this form for submitting comments. Use the [electronic form](https://sbs.nerc.net/) to submit comments on proposed **CIP-013-1 − Cyber Security - Supply Chain Risk Management**. The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, March 6, 2017**.

Documents and information about this project are available on the [project page](http://www.nerc.com/pa/Stand/Pages/Project201603CyberSecuritySupplyChainManagement.aspx). If you have any questions, contact Standards Developer, [Mark Olson](mailto:mark.olson@nerc.net) (via email), or at (404) 446-9760.

## Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued [Order No. 829](http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order_SupplyChain_20160721_RM15-14.pdf) directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

"[The Commission directs] NERC to develop a forward-looking, objective-based 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. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed proposed CIP-013-1 to address the above directives.

## Questions

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Yes

No

Comments:

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Yes

No

Comments:

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Yes

No

Comments:

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Yes

No

Comments:

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Yes

No

Comments:

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

Yes

No

Comments:

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

Yes

No

Comments:

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

Yes

No

Comments:

9. Provide any additional comments for the SDT to consider, if desired.

Comments: