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 the following proposed standards:

* CIP-013-1 – Cyber Security – Supply Chain Risk Management
* CIP-005-6 – Cyber Security – Electronic Security Perimeter(s)
* CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments

The electronic comment form must be completed by **8:00 p.m. Eastern, Thursday, June 15, 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 Senior Standards Developer, Mark Olson (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 the proposed standard and modifications to approved standards 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 has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

[ ]  Yes

[ ]  No

Comments:

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

[ ]  Yes

[ ]  No

Comments:

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 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). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

[ ]  Yes

[ ]  No

Comments:

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT’s removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

[ ]  Yes

[ ]  No

Comments:

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

[ ]  Yes

[ ]  No

Comments:

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

[ ]  Yes

[ ]  No

Comments:

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC’s [Compliance Guidance policy](http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf) for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

[ ]  Yes

[ ]  No

Comments:

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

[ ]  Yes

[ ]  No

Comments:

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

Comments: