Unofficial Comment Form
Project 2016-03 Cyber Security Supply Chain Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on the Standards Authorization Request (SAR) developed by NERC Staff. The electronic comment form must be completed by 8:00 p.m. Eastern, Friday, November 18, 2016.

Documents and information about this project are available on the project page. If you have any questions, contact 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 that directed 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."

The Commission also directed the new or revised Standard to be filed within one-year of the effective date of the Order.

The drafting team has developed a SAR for new or modified Critical Infrastructure Protection (CIP) Standard(s) to require applicable entities to develop and implement plan(s) that include security controls for supply chain management of industrial control system hardware, software, and computing and networking services that impact BES operations as described in Order No. 829.

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. Do you agree with the proposed scope for Project 2016-03 as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

☐ Yes
☒ No

Comments:
We have suggestions on
1) Purpose,
2) Industry Need,
3) Brief Description
4) Detailed Description to better define this project’s scope.

For Purpose, we have three recommendations
A) change “supply chain management” to “supply chain risk management”;  
B) change “and implement a plan that includes security controls for supply chain management for” to “and implement measures for supply chain risk management for”;  
C) copy the final industry need sentence to the Purpose – “The new or modified Reliability Standard(s) is intended to reduce the risk of a cyber security incident affecting the reliable operation of the Bulk-Electric System.”

Supply chain management is the flow of goods, services and resources that involve the movement, storage and maintenance of material for work in progress. Supply chain risk management is a subset of supply chain management. For this SAR, supply chain risk management should focus on the risks associated with sourcing and servicing BES Cyber System Components from external entities.

For Industry Need, we have one recommendation – change “On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven new or modified Reliability Standard(s) that addresses” to “On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven, risk-based new or modified Reliability Standard(s) that addresses”

For Brief Description, we have one recommendation – update the Brief Description to be consistent with our proposed changes to the Purpose and Industry Need.

For Detailed Description, we have one recommendation – change “The plan may apply different controls based on the criticality of different assets (Order No. 829 at P44)” to “The plan may apply different measures based on the criticality of different assets (Order No. 829 at P44)”

2. Provide any additional comments for the Standards Drafting Team to consider, if desired.
Comments:
We also recommend that the SDT seriously consider updating existing CIP Standards in order to avoid creating double jeopardy for
   A) remote access (CIP-005 R2);
   B) patch management (CIP-007 R2);
   C) authentication (CIP-007 R5);
   D) vendor termination of employees (CIP-004 R5);
We recommend that new Requirements do not jeopardize existing Requirements and their implementation timelines, and that new Requirements do not create additional paperwork with little value to the Reliable Operation of the Bulk Electric System.