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

DO NOT use this form for submitting comments. Use the electronic form to submit comments on the following proposed standards:

- 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](#). If you have any questions, contact Senior Standards Developer, [Mark Olson](mailto:mark.olson@nerc.com) (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued [Order No. 829](#) 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:
Concerned that the R1 guidance provides details which are beyond the scope of R1

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).
Recommend removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it?
   - What is implied by (ii) transitions from one vendor(s) to another vendor(s)? Why is this distinction necessary? Wouldn’t a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?
   - R1.2.2: “Coordination of responses to vendor-identified incidents….”, it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.

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:
The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question.
Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-013.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

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:

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection.

Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions:

- How does one prove that a method is not available?
- What is the line between available/unavailable? How far do you have to go?
We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.

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:
None
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:
Recommend changing this General Consideration from
Contracts entering the Responsible Entity’s procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To
Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note

Implementation Plan does not handle unplanned changes such as IROLs or registration, etc.

Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards

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:
None
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 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:
Implementation Guidance for R3
Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:”

Implementation Guidance for R3 –
Recommend removing this language from the second main bullet, since it is beyond the Requirement “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”

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:
No comment

9. Provide any additional comments for the SDT to consider, if desired.
Comments:
No comment