Unofficial Comment Form

Supply Chain Risk Assessment Data Request

**DO NOT** use this form for submitting comments. Use the [electronic form](https://nerc.checkboxonline.com/F9C84202-1A5C-41F1-A963-6864BB5DEB48) to submit comments on proposed **Request for Data or Information Supply Chain Risk Assessment Data Request (Supply Chain Data Request).** The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, July 22, 2019**.

Documents and information are available on the Supply Chain Risk Mitigation Program [initiative page](https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx). If you have any questions, contact [Howard Gugel](mailto:howard.gugel@nerc.net?subject=1600%20Data%20Request%20question), Vice President of Engineering and Standards, by email or at (404) 446-9693.

## Background Information

In 2017, NERC developed new and revised critical infrastructure protection (CIP) Reliability Standards to help mitigate cyber security risks associated with the supply chain for high and medium impact Bulk Electric System (BES) Cyber Systems. These standards, collectively referred to as Supply Chain Standards, consist of new Reliability Standard CIP-013-1 and revised Reliability Standards CIP-010-3 and CIP-005-6. Consistent with the risk-based framework of the NERC CIP Reliability Standards, the Supply Chain Standards will be applicable to the highest-risk systems that have the greatest impact to the grid. The Supply Chain Standards will require entities that possess high and medium impact BES Cyber Systems to develop processes to ensure responsible entities manage supply chain risks to those systems through the procurement process, thereby reducing the risk that supply chain compromise will negatively impact the BPS.

When adopting the Supply Chain Standards in August 2017, the NERC Board of Trustees (Board) directed NERC to undertake further action on supply chain issues. Among other things, the Board directed NERC to study the nature and complexity of cyber security supply chain risks, including those associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address identified risks.

In its final report accepted by the NERC Board in May 2019,[[1]](#footnote-1) NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks. NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with External Routable Connectivity by issuing a Request for Data or Information pursuant to Section 1600 of the NERC Rules of Procedure. NERC staff worked with the Critical Infrastructure Protection Committee (CIPC) Supply Chain Working Group (SCWG) to develop the questions in this data request.

Given that this is a request for data or information that must be obtained in order to evaluate a threat to the reliability or security of the BPS, NERC is issuing this request for data or information in accordance with the expedited timing provisions of Section 1606 of the NERC Rules of Procedure. On June 13, 2019, the Board authorized the use of shortened review and comment periods. NERC provided this data request to the FERC Office of Electric Reliability for information on June 24, 2019. NERC posted this data request for public comment for a twenty (20) day comment period from July 2—July 22, 2019. In accordance with Section 1600 of the NERC Rules of Procedure, this data request is mandatory for U.S. entities. Although not required, Canadian registered entities are encouraged to participate.

## 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. NERC and the SCWG developed the proposed Rules of Procedure Section 1600 Request for Data or Information Supply Chain Risk Assessment Data Request (Supply Chain Data Request) to assist in determining whether the inclusion of low impact BES Cyber Systems with external routable connectivity should be considered while taking into account the number and nature of such low impact BES Cyber Systems, the benefits of including such systems in the Supply Chain Standards, and the associated costs of extending CIP-013 to cover these systems. Do you agree that the proposed Supply Chain Data Request describes the data necessary to determine whether low impact BES Cyber Systems with external routable connectivity should be considered? If you do not agree, or if you agree but have comments or suggestions for the Supply Chain Data Request provide your recommendation and explanation.

Yes

No

Comments:

2. The Reporting Entities for the Supply Chain Data Request are all registered entities that are required to comply with CIP-002-5.1a. Do you agree that these are the correct Reporting Entities for the Supply Chain Data Request? If you do not agree, or if you agree but have comments or suggestions for the Reporting Entities specified in the Supply Chain Data Request provide your recommendation and explanation.

Yes

No

Comments:

3. The proposed Supply Chain Data Request has a due date of 45 days following the date of issuance of the data request. This time frame was set to allow the analysis of the data to be presented at the NERC Board of Trustees November 2019 meeting. Will your organization be able to complete the data request in 45 days? If you do not agree, or if you agree but have comments or suggestions for an alternative time frame provide your recommendation and explanation.

Yes

No

Comments:

4. NERC does not anticipate that the requested information specified in the Supply Chain Data Request will contain Confidential Information as that term is defined in Section 1501 of the NERC Rules of Procedure. Do you agree? If you do not agree, specify the type of data that is being requested in the proposed Supply Chain Data Request, and the justification for its classification as Confidential Information under Section 1501 of the NERC Rules of Procedure.

Yes

No

Comments:

5. Provide any additional comments for NERC staff and the SCWG to consider, if desired.

Comments:

1. NERC’s final Supply Chain report can be found at: <https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf> [↑](#footnote-ref-1)