NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Request for Data or Information

Supply Chain Risk Assessment Data Request

~~Draft~~

August ~~xx~~19, 2019

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

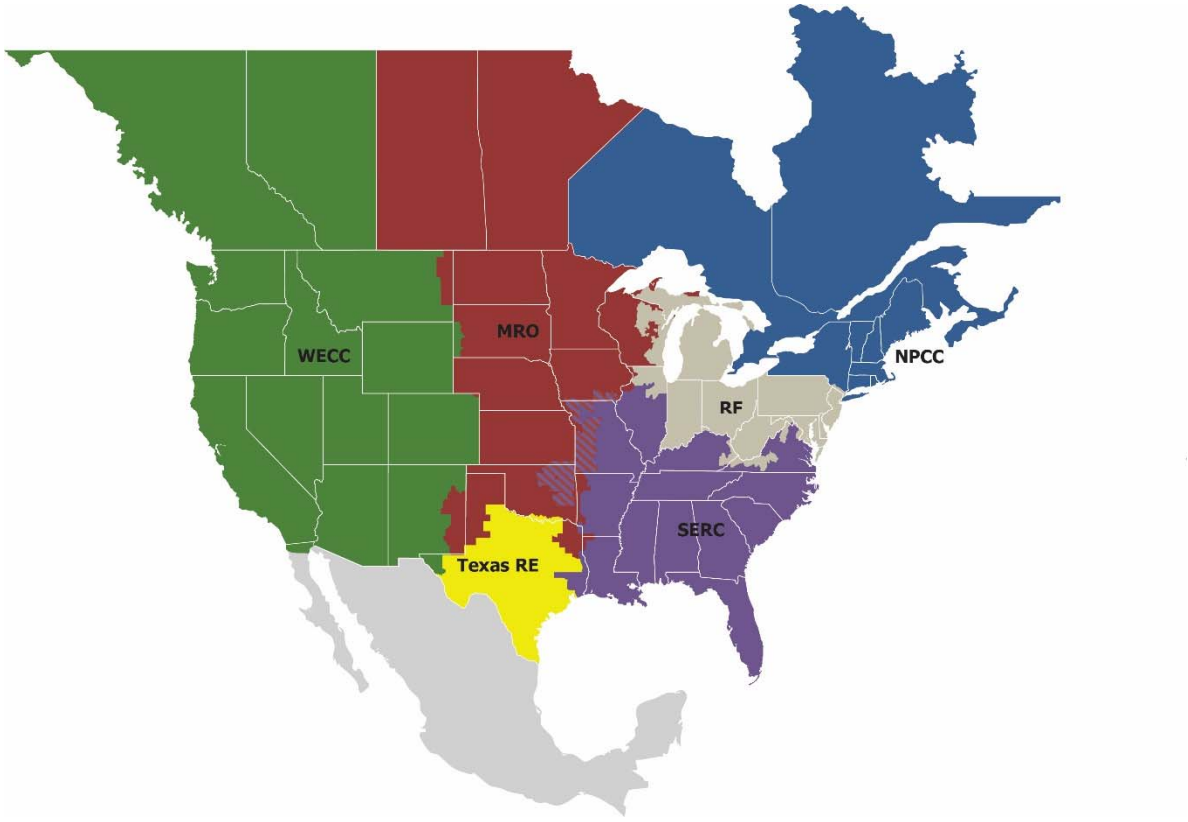
Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security

Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

In accordance with Section 1600 of the NERC Rules of Procedure,[1] NERC may request data or information that is deemed necessary to meet its obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of the Federal Energy Regulatory Commission's ("FERC") regulations. This is such a request.

This request was developed in accordance with the expedited procedures provided in Section 1606 of the NERC Rules of Procedure. Section 1606 allows for a shortened time period for posting a draft request for data or information for comment if the data or information must be obtained in order to evaluate a threat to the reliability or security of the BPS or in order to comply with a directive in an order issued by FERC or another governmental authority.

Background

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,[2] 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 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. The Board approved the formal issuance of this data request on August xx, 2019. Accordingly, in accordance with Section 1600 of the NERC Rules of Procedure, this data request is mandatory for U.S. entities. Owners. Although not required, Canadian registered entities are encouraged to participate.

[1] NERC's Rules of Procedure are available at: https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20180719.pdf

[2] 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

Due Date and NERC Contact Information

The completion of this data request and submission to NERC is due within forty-five days after receipt of the data request. Please complete the data request using the following website:

http…….{to be inserted}

Any other questions may be directed to Howard Gugel at: howard.gugel@nerc.net or by telephone at 404.446.9693.

Authority

Section 215 of the Federal Power Act

Under Section 215 of the Federal Power Act (16 U.S.C. § 824o), Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the nation's BPS, and with the duties of certifying an Electric Reliability Organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. NERC was certified as the ERO on July 20, 2006. NERC's authority for issuing this data request is derived from Section 215 of the Federal Power Act, and from the following sources:

NERC is requesting this information in accordance with its authority provided in 18 C.F.R. §39.2(d), which provides:

> *Each user, owner or operator of the Bulk-Power System within the United States (other than Alaska and Hawaii) shall provide the Commission, the Electric Reliability Organization and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission and set out in the Rules of the Electric Reliability Organization and each applicable Regional Entity. The Electric Reliability Organization and each Regional Entity shall provide the Commission such information as is necessary to implement section 215 of the Federal Power Act.*

NERC Rules of Procedure

Additionally, NERC Rules of Procedure Section 1600 provides in pertinent part:

> ***1601. Scope of a NERC or Regional Entity Request for Data or Information***
> *Within the United States, NERC and Regional Entities may request data or information that is necessary to meet their obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of the Commission's regulations, 18 C.F.R. § 39.2(d). In other jurisdictions NERC and Regional Entities may request comparable data or information, using such authority as may exist pursuant to these Rules of Procedure and as may be granted by Applicable Governmental Authorities in those other jurisdictions. The provisions of Section 1600 shall not apply to Requirements contained in any Reliability Standard to provide data or information; the Requirements in the Reliability Standards govern. The provisions of Section 1600 shall also not apply to data or information requested in connection with a compliance or enforcement action under Section 215 of the Federal Power Act, Section 400 of these Rules of Procedure, or any procedures adopted pursuant to those authorities, in which case the Rules of Procedure applicable to the production of data or information for compliance and enforcement actions shall apply.*
>
> ***1602. Procedure for Authorizing a NERC Request for Data or Information***
>
> *****
>
> *2.1. A proposed request for data or information shall contain, at a minimum, the following information: (i) a description of the data or information to be requested, how the data or information will be used, and how the availability of the data or information is necessary for NERC to meet its obligations under applicable laws and agreements; (ii) a description of how the data or information will be collected and validated; (iii) a description of the entities (by functional class and jurisdiction) that will be required to provide the data or information ("Reporting Entities"); (iv) the schedule or due date for the data or information; (v) a description of any restrictions on disseminating the data or information (e.g., "Confidential Information," "Critical Energy Infrastructure Information," "aggregating" or "identity masking"); and (vi) an estimate of the relative burden imposed on the Reporting Entities to accommodate the data or information request.*

2.2. *A proposed modification to a previously authorized request for data or information shall explain (i) the nature of the modifications; (ii) an estimate of the burden imposed on the Reporting Entities to accommodate the modified data or information request, and (iii) any other items from Section 1602.2.1 that require updating as a result of the modifications.*

3. *After the close of the comment period, NERC shall make such revisions to the proposed request for data or information as are appropriate in light of the comments. NERC shall submit the proposed request for data or information, as revised, along with the comments received, NERC's evaluation of the comments and recommendations, to the Board of Trustees.*

4. *In acting on the proposed request for data or information, the Board of Trustees may authorize NERC to issue it, modify it, or remand it for further consideration.*

5. *NERC may make minor changes to an authorized request for data or information without Board approval. However, if a Reporting Entity objects to NERC in writing to such changes within 21 days of issuance of the modified request, such changes shall require Board approval before they are implemented.*

6. *Authorization of a request for data or information shall be final unless, within thirty (30) days of the decision by the Board of Trustees, an affected party appeals the authorization under this Section 1600 to the Applicable Governmental Authority.*

1606. Expedited Procedures for Requesting Time-Sensitive Data or Information

1. *In the event NERC or a Regional Entity must obtain data or information by a date or within a time period that does not permit adherence to the time periods specified in Section 1602, the procedures specified in Section 1606 may be used to obtain the data or information. Without limiting the circumstances in which the procedures in Section 1606 may be used, such circumstances include situations in which it is necessary to obtain the data or information (in order to evaluate a threat to the reliability or security of the Bulk Power System, or to comply with a directive in an order issued by the Commission or by another Applicable Governmental Authority) within a shorter time period than possible under Section 1602. The procedures specified in Section 1606 may only be used if authorized by the NERC Board of Trustees prior to activation of such procedures.*

2. *Prior to posting a proposed request for data or information, or a modification to a previously-authorized request, for public comment under Section 1606, NERC shall provide the proposed request or modification, including the information specified in paragraph 1602.2.1 or 1602.2.2 as applicable, to the Commission's Office of Electric Reliability. The submission to the Commission's Office of Electric Reliability shall also include an explanation of why it is necessary to use the expedited procedures of Section 1606 to obtain the data or information. The submission shall be made to the Commission's Office of Electric Reliability as far in advance, up to twenty-one (21) days, of the posting of the proposed request or modification for public comments as is reasonably possible under the circumstances, but in no event less than two (2) days in advance of the public posting of the proposed request or modification.*

3. *NERC shall post the proposed request for data or information or proposed modification to a previously-authorized request for data or information for a public comment period that is reasonable in duration given the circumstances, but in no event shorter than five (5) days. The proposed request for data or information or proposed modification to a previously-authorized request for data or information shall include the information specified in Section 1602.2.1 or 1602.2.2, as applicable, and shall also include an explanation of why it is necessary to use the expedited procedures of Section 1606 to obtain the data or information.*

4. *The provisions of Sections 1602.3, 1602.4, 1602.5 and 1602.6 shall be applicable to a request for data or information or modification to a previously-authorized request for data or information developed and issued pursuant to Section 1606, except that (a) if NERC makes minor changes to an authorized request*

for data or information without Board approval, such changes shall require Board approval if a Reporting Entity objects to NERC in writing to such changes within five (5) days of issuance of the modified request; and (b) authorization of the request for data or information shall be final unless an affected party appeals the authorization of the request by the Board of Trustees to the Applicable Governmental Authority within five (5) days following the decision of the Board of Trustees authorizing the request, which decision shall be promptly posted on NERC's website.

How the data will be used

The data will be used by NERC staff to assist in determining whether the inclusion of low impact BES Cyber Systems with inbound or outbound electronic access, as defined in CIP-003-7, Attachment 1, Section 3, ~~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.

NERC will publish a summary assessment of results of this data request. Individual registered entity responses will not be published.

Why the data is necessary

The availability of the data and information is necessary for NERC to meet its obligations under applicable laws and agreements. The Energy Policy Act of 2005 mandates the development of Reliability Standards that provide for the reliable operation of the BPS, including cyber security protection. This data request is being developed to support the ongoing evaluation of the Supply Chain Standards, which directly supports the statutory responsibility from the Energy Policy Act to ensure the reliable operation of the BPS, including cyber security protection. The purpose of this data request is to determine the risk to the BES presented by not including low impact BES Cyber Systems in the Supply Chain Standards, including gathering information on how existing risks are being mitigated.

How the data will be collected and validated

NERC ~~will~~ has ~~identify~~ identified the registered entities necessary to complete the survey, which are provided below. NERC will use its Checkbox survey tool to prepare the survey and provide instruction to the registered entities to submit the data. NERC will compare the list of registered entities with the data request respondents to ensure that responses are received as requested.

Reporting Entities

- Balancing Authorities
- Distribution Providers
- Generator Owners
- Generator Operators
- Reliability Coordinators
- Transmission Owners
- Transmission Operators

Due date for the information

Reporting entities are expected to respond to the data request within 45 days of its issuance.

Restrictions on disseminating data (Confidential/CEII)

NERC is not requesting specific information relative to BES Cyber Systems that would create the need to invoke critical energy infrastructure confidentiality provisions. NERC is treating all responses to this data request as non-public information. Additionally, NERC does not intend to publish entity specific information collected through this data request. Only data in summary fashion will be made publicly available.

NERC, however, is not requesting specific information relative to BES Cyber Systems that would create the need to invoke Confidential Information/Critical Energy Infrastructure Information protections under Section 1500 of the NERC Rules of Procedure.

Estimate on burden imposed to collect data

This is a one-time data request using in part the results analysis required under current CIP-002-5.1a. The incremental burden for this one-time data collection will be the effort required to estimate the number of low impact BES Cyber systems, the number of those containing inbound or outbound electronic access, as defined in CIP-003-7, Attachment 1, Section 3~~external routable connectivity~~, and the location risk score for low impact BES Cyber Systems. The estimated time to complete the data request will vary with the size of the entity, but is estimated to average less than 100 hours total per entity.

Data Request

Supply Chain Risk Assessment Data Request

(Note: this information will be converted to the electronic survey tool to be implemented upon approval of this Data Request)

In its May 17, 2019 report entitled "Cyber Security Supply Chain Risks – Staff Report and Recommended Actions," (the "Supply Chain Report"), NERC recommended issuing a data request under Section 1600 of the NERC Rules of Procedure "to obtain more information about the nature and number of BES Cyber Systems currently in use." This report states that the data request would include questions "to determine the incremental costs and potential benefits to extend CIP-013 to low impact BES Cyber Systems with External Routable Connectivity." This data request is intended to achieve the objectives stated in the Supply Chain Report.

General Questions:

1. What are the NERC Compliance Registry (NCR) numbers for which you are reporting under this Data Request?
2. Entity contact information
    a. Name:
    b. Title:
    c. Email address:
    d. Contact number:

BES Cyber Systems:

Objective: To quantify and classify the number of assets containing low impact BES Cyber Systems, specifically those that have inbound or outbound electronic access, as defined in CIP-003-7, Attachment 1, Section 3~~external routable connectivity~~, to holistically quantify risk and determine gaps between those assets covered by CIP-013 and those that are not.

The following information is provided to assist in answering Questions 3 through 5.

In order for NERC to understand the data they receive from this Data Request, they need to understand the basis for each entity's answer. This means that how your entity categorized your BES Cyber Systems can have a huge impact on these survey results. In order to have Data Request results that can be used and compared, the common basis are the six locations called out in CIP-002. This Data Request is focused on those locations and not how entities have designed their BES Cyber Systems.

In NERC's "Supply Chain Risks and Recommended Actions" report, NERC staff expects: (1) entities that have medium or high impact BES Cyber Systems to voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems; and (2) entities that own only low impact BES Cyber Systems to develop supply chain risk management programs tailored to their unique risk profiles and priorities.

The term "location"[3] refers to physical space associated with an asset (as defined in Footnote 3 of this data request). A location includes any number of BES Cyber Systems at a given asset, as defined in CIP-002-5.1a, that operate at a

[3] CIP-002-5.1a, Requirement R1 identifies six types of "assets" that entities must consider: (i) Control Centers and backup Control Centers; (ii) Transmission stations and substations; (iii) Generation resources; (iv) Systems and facilities critical to system restoration; (v) Special Protection Systems; (vi) for Distribution Providers, Protection Systems specified in CIP-002-5.1a, Applicability Section 4.2.1. For the purpose of this data request, the word "asset" is used in the same way as it is used in CIP-002-5.1a Requirement R1. The capitalized term "Cyber Asset" is used in this Data Request to have the same meaning as it has in the NERC Glossary of Terms.

common Impact Rating. For example, if a substation contains both medium and low impact BES Cyber Systems, you would include it in both counts. For question 3, low impact count is all low impact assets containing BES Cyber Systems, including those with external connectivity.[4] For each location in the response to ~~Question~~ question ~~46~~, ~~list the~~provide an estimate of the low impact assets identified pursuant to CIP-002 R 1.3.

3. CIP-002 Classifications

	Number of assets containing BES Cyber Systems
High/Medium impact w/ ERC:	
Medium impact without ERC:	
Low impact:	
Low impact with ~~erc~~external connectivity[4]:	

4. If you have medium or high impact BES Cyber Systems, please explain how your ~~plans to apply~~ CIP-013-1 R1 plan will affect ~~to~~ your low impact BES Cyber Systems and describe methods (if any) you intend to use to apply your plan to low impact BES Cyber Systems. In addition, have you determined if there are supply vendors used for acquiring low impact BES Cyber Assets that don't provide similar equipment or services to your high or medium impact BES Cyber Assets? If yes, please describe how you intend to address the risk:

5. If you have only low impact BES Cyber Systems, briefly explain how you currently plan on mitigating Supply Chain Management risks:

The following information is provided to assist in answering question 6.

In order to help NERC determine the risk to the BES associated with each of the locations containing low impact BES Cyber Systems, a scoring system based on the characteristics of the assets at that location has been developed. Note that because low impact BES Cyber Systems are understood to pose some kind of risk to the BES, '1' is the lowest score on the scale. Neither the CIP Version 5 Reliability Standards nor the data request require entities to have an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets. -To complete the data request related to low impact BES Cyber Assets, an entity need only identify, to the best of its ability, the locations of low impact Cyber Assets and provide an approximate number of those locations. For each location

[4] In this context, the phrase "external ~~routable~~ connectivity" refers to inbound or outbound electronic access, as defined in ~~the requirements under~~ CIP-003-7, Attachment 1, Section 3. This is not to be confused with External Routable Connectivity that applies to medium and high impact BES Cyber Systems.

containing different or multiple assets, use the first criterion that applies (i.e., count each location once) in the below chart to determine its associated risk score:[5]

Location Risk Score Table			
Criterion (See CIP-002 Attachment 1)	**Description**	**Risk Criterion**	**Location Risk Score**
3.1	Control Centers / backup Control Centers[6]	MW of load and/or generation cControlled	0-500 MW = 2 501-1000 MW = 3 1001 - 1500 MW = 4
3.2	Transmission stations and substations	MVA/Criterion 2.5 Score	0-1400 = 2 1401 - 2000 = 3 2001 - 3000 = 4
3.3	Generation resources[7]	MW per location	0-500 MW = 2 501-1000 MW = 3 1001 - 1500 MW = 4
3.4	Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements[8] if not counted in 3.2 or 3.3	All locations will receive the same score.	2
3.5	SPS/RAS that support the reliable operation of the BES if not counted in 3.2 or 3.3	All locations will receive the same score.	2
3.6	For DPs, Protection Systems specified in Applicability section 4.2.1 if not counted in 3.2 or 3.3	All locations will receive the same score.	1

~~4.~~6. For each location identified, please answer the following questions. You may group assets with the same answers into a single line item. Note "inbound or outbound connectivity~~external routable connectivity~~" refers to the requirements under CIP-003-7, Attachment 1, and Section 3. This is not to be confused with External Routable Connectivity that applies to medium and high impact BES Cyber Systems.

Impact Categorization BES Cyber Systems (See CIP-002, Attachment 1)	3.1			3.2			3.3			3.4	3.5	3.6
Location Risk Score[9]	2	3	4	2	3	4	2	3	4	2	2	1

[5] An example response is provided as an attachment to assist in completing question 5

[6] These are low impact Control Centers per CIP-002-5.1a which only apply to some BAs and GOPs.

[7] If your entity has performed generation segmentation and created multiple low impact BES Cyber Systems, please account for them as individual low impact BESCS locations (4 units would count as 4 locations) as per your CIP-002. Don't double-count under medium impact under question 3 and again as low impact under question 5.

[8] If this includes generation counted under 3.3, do not count again under 3.4

[9] Risk score is based off of the value found in the "Location Risk Score Table" above

a. -Number of locations with low impact BES Cyber Systems												
b. Number of locations with inbound or outbound connectivity~~external routable connectivity~~ to a BES Cyber System												
c. Number of locations with dial up connectivity to a BES Cyber System												
d. Number of locations allowing third party remote access[10] to a BES Cyber System												
e. Number of locations with third party monitoring of ~~the asset to~~ a BES Cyber System[11]												
f. Number of locations with constant monitoring[12] of remote connectivity to a BES Cyber System												
g. Number of locations participating in government/industry programs[13]												
h. Number of locations with NO external routable connectivity and NO dial up connectivity to a BES Cyber System												

CIP-013 Cost of Implementation:

The following information should be used when answering the questions after the information:

Stakeholders, regulators and legislator's decisions on mitigating and preventing supply chain risks depend on the costs and benefits associated with those decisions. While utilities would want and share this information, it is not currently available. Therefore, subject matter experts believe it is premature for CIP-013 registered entities to determine, or estimate costs or benefits associated with the implementation of the standard.

- The standard is new and there is no historic precedence for registered entities to pre-determine costs based on furthering relationships with existing and new vendors.

[10] Access, for the purpose of this data request, means communication other than outward bound data (e.g. a data diode that only sends data out of the location would not count).

[11] Third party monitoring refers to connections that send data to an OEM or other third party that monitors components at this location for performance, maintenance or other such reasons.

[12] Constant monitoring, for the purpose of this data request, means the ability to monitor connectivity and the ability to disconnect remote connectivity if malicious activity is detected.

[13] Government/Industry programs include, but are not limited to, CRISP, CYOTE and/or Neighborhood Keeper. If a registered entity participates in one or more of these programs, they should only include the locations that are participating in the program. For example, do not count locations where the program(s) are applied only at a non-CIP environment (e.g., corporate).

- These costs and benefits are intangible and depend on a spectrum of actions, from internal process refinement costs to extensive costs associated with replacement of blacklisted vendors.
- The cost of compliance is currently unknown as this is a new standard.
- Many utilities are experiencing push back from vendors for CIP-013 compliance that could require vendor change or increase in cost from such vendors.

Consequently, CIP-013 is causing, and will necessitate many changes for complying utilities from now until the July 1, 2020 implementation date. Therefore, currently providing any credible cost or benefit information is premature.

~~5.~~7. Do you agree with the above SME assessment – Yes or No?

Please provide CIP-013 cost or benefit amounts should you answer “no” to the above question:

Example Response

Due to the complex nature of the NERC CIP standards, the variety of ways an entity can classify their own Cyber Assets, and the desire to have as comparable data as possible, this example is intended to help entities understand the questions and how to formulate responses.

Example:
Happy Valley Power (HVP) is a medium-sized utility. They have all classifications of BES Cyber Systems. Using their current CIP-002 evidence, they review what they have in order to respond to the Data Request. They have:

- A high impact Control Center/Backup Control Center (with data centers that are considered to be the same BES Cyber System)
- Three medium impact substations. They already have plans to put all of their transmission and EMS systems through their future CIP-013 plans, however they are not ready to do this for their generation equipment
- A few Remedial Action Schemes that provide protection for both BES and non-BES Elements
- A fair number of locations containing low impact BES Cyber Systems (both transmission and generation). Generally speaking, HVP groups their BES Cyber Systems per asset. HVP does not have an inventory of their BES Cyber Assets at their generation plants.

HVP has reviewed the Data Request and decided to organize their information in the best way possible to help answer the request quickly and efficiently. HVP understands that one of the goals of the Data Request is to avoid double-counting assets, and so they will process their assets in the order of the table in question ~~5~~6.

HVP understands that there can be confusion between the various terms used by NERC CIP-002 as well as by others in the industry. They have read over the Data Request and understand the need to collect the data in an organized fashion. The Data Request is focused on "locations". These locations are another way of saying "asset" per CIP-002-5.1a R1, but in order to avoid confusion between "asset", "Cyber Asset" and "BES Cyber Asset", the Data Request uses the term "location".

Here's HVP's answer to question 3 & 4 on the Data Request:

3. CIP-002 Classifications

	Number of assets containing BES Cyber Systems
High/Medium impact w/ ERC:	4
Medium impact without ERC:	0
Low impact:	28
Low impact with ~~erc~~[4]external connectivity[4]:	26

4. If you have medium or high impact BES Cyber Systems, please explain how your ~~plans to apply~~ CIP-013-1 R1 plan will affect ~~to~~ your low impact BES Cyber Systems and describe methods (if any) you intend to use to apply your plan to low impact BES Cyber Systems. In addition, have you determined if there are supply vendors used for acquiring low impact BES Cyber Assets that don't provide similar equipment or services to your high or medium impact BES Cyber Assets? If yes, please describe how you intend to address the risk:

HVP plans on applying CIP-013 R1 controls to any devices at a low impact substation as well as the medium & high impact BES Cyber Systems as required by CIP-013. HVPs investigating the costs associated with applying R1 to generation sites. HVP has not identified any supply vendors used for acquiring low impact BES Cyber Assets that don't provide similar equipment or services to our high or medium impact BES Cyber Assets

5. If you have only low impact BES Cyber Systems, briefly explain how you currently plan on mitigating Supply Chain Management risks:
Not applicable

HVP now looks at the risk table to determine how many categories they have to answer for under question ~~5~~6. Here's the table from the Data Request for locations:

Location Risk Score Table			
Criterion (See CIP-002 Attachment 1)	**Description**	**Risk Criterion**	**Location Risk Score**
3.1	Control Centers / backup Control Centers~~65~~	MW of load and/or generation c~~C~~ontrolled	0-500 MW = 2 501-1000 MW = 3 1001 - 1500 MW = 4
3.2	Transmission stations and substations	MVA/Criterion 2.5 Score	0-1400 = 2 1401 - 2000 = 3 2001 - 3000 = 4
3.3	Generation resources~~76~~	MW per location	0-500 MW = 2 501-1000 MW = 3 1001 - 1500 MW = 4
3.4	Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements~~87~~ if not counted in 3.2 or 3.3	All locations will receive the same score.	2
3.5	SPS/RAS that support the reliable operation of the BES if not counted in 3.2 or 3.3	All locations will receive the same score.	2
3.6	For DPs, Protection Systems specified in Applicability section 4.2.1 if not counted in 3.2 or 3.3	All locations will receive the same score.	1

For HVP, this is how their 28 LIBCS break down:

19 are substations
4 are RAS
5 are generation plants

For the substations, most of them are under the 200kV threshold for criterion 2.5. However, a few are not. They have 5 substations that have ratings at various levels:

Sub 1: 1 345kV line, 1 230kV line, 5 115kV lines (Criterion 2.5 score = 2000, Location Risk Score = 3)
Sub 2: 1 345kV line, 2 230kV lines, 4 115kV lines (Criterion 2.5 score = 2700, Location Risk Score = 4)
Sub 3: 3 230kV lines, 6 115kV lines (Criterion 2.5 score = 2100, Location Risk Score = 4)
Sub 4: 1 230kV line, 8 115kV lines (Criterion 2.5 score = 300, Location Risk Score = 2)
Sub 5: 1 345kV line, 6 115kV lines (Criterion 2.5 score = 1300, Location Risk Score =2)

HVP's other 14 substations do not have lines above 200kV, and therefore do not rank on the criterion 2.5 chart. However, they are low impact and score a "0" on criterion 2.5, so are therefore a Location Risk Score of 2. So HVP has:

16 substations with a Location Risk Score of 2,
1 substation with a Location Risk Score of 3, and
2 substations with a Location Risk Score of 4.

HVP's 5 generation plants are of various size as well:

Plant 1 is an aggregate 1200MW (Location Risk Score = 4)
Plant 2 is an aggregate 725MW (Location Risk Score = 3)
Plant 3 is a single unit, 800MW (Location Risk Score = 3)
Plant 4 is an aggregate 450MW (and also a Black Start unit) (Location Risk Score = 2)
Plant 5 is an aggregate 1200MW (Location Risk Score = 4)

For RAS, all of HVP's RAS are located at substations that are already accounted for under the 3.2 scoring of locations, so they will not count them again under 3.4.

Since HVP's Black Start unit is counted under 3.3, they will not count it again under 3.5.

HVP now looks at each of these locations, and starts with section 3.1 – Control Centers. HVP does not have any low impact Control Centers, so that nets out a '0' for all areas under 3.1.

Next is 3.2 (substations).
They have "external routable connectivity" for their own SCADA use, but do not allow any third party remote access of any kind to any substation. HVP fills out section 3.2 accordingly (recall they have 16 substations with a Location Risk Score of 2, one substation with a Location Risk Score of 3, and two substations with a Location Risk Score of 4). They then fill these numbers in on the sheet under section 3.2.

For 3.3, HVP has the following plants:

Plant 1 is an aggregate 1200MW (4 units, 500MW, 300MW, 250MW and 150MW). Because there are different vendors at this one location, some units have monitoring and other do not. Remote access is allowed via an as-needed basis through a two factor authentication that's managed by the operators at the plant. However, scoring is based off of allowing remote access to any BES Cyber System at that location, so all units are treated the same for the purpose of this Data Request. This location counts under a, b, d, e and f.

Plant 2 is an aggregate 725MW. It has remote monitoring and they monitor the remote access into the facility. This location counts under a, b, d and f.

Plant 3 is a single unit, 800MW. It has monitored remote access. This location counts under a, b, d and f.

Plant 4 is an aggregate 550MW – there is a data diode here for sending out plant data, but no remote access/connectivity. It is also a Black Start capable unit. This location counts under a and h in the table.

Plant 5 is an aggregate 1200MW, and along with monitoring of the remote access, they are also involved in the Neighborhood Keeper program. This location counts under a, b, d, e, g and f.

Due to double-counting, HVP does not have anything that counts under 3.4 and 3.5. HVP also does not qualify for anything under 3.6.

HVP's final answers look like this:

Impact Categorization BES Cyber Systems (See CIP-002, Attachment 1)	3.1			3.2			3.3			3.4	3.5	3.6
Location Risk Score[9] ~~8~~	2	3	4	2	3	4	2	3	4	2	2	1
a. ~~-~~Number of locations with low impact BES Cyber Systems	0	0	0	16	1	2	1	2	2	0	0	0
b. Number of locations with inbound or outbound connectivity ~~external routable connectivity~~ to a BES Cyber System	0	0	0	16	1	2	1	2	2	0	0	0
c. Number of locations with dial up connectivity to a BES Cyber System	0	0	0	0	0	0	0	0	0	0	0	0
d. Number of locations allowing third party remote access[10] to a BES Cyber System	0	0	0	0	0	0	0	2	2	0	0	0
e. Number of locations with third party monitoring of ~~the asset to~~ a BES Cyber System[11] ~~9~~	0	0	0	0	0	0	0	1	0	0	0	0
f. Number of locations with constant monitoring[12] of remote connectivity to a BES Cyber System	0	0	0	0	0	0	0	2	2	0	0	0
g. Number of locations participating in government/industry programs[13] ~~10~~	0	0	0	0	0	0	0	0	1	0	0	0
h. Number of locations with NO external routable connectivity and NO dial up connectivity to a BES Cyber System	0	0	0	0	0	0	1	0	0	0	0	0