NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Response to Comments
Supply Chain Risk Assessment Data Request

Questions
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.
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.
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.

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

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.

Submitter Name	Submitter Company	Answer/Comment
Todd Candler	General Electric	Yes
Response		
Thank you for your response.		
Robert Gray	Board of Public Utilities (Kansas City KS) (BPU)	Yes
Response		
Thank you for your response.		
Kjersti Drott	Tri-State Generation and Transmission Assoc., Inc.	Yes
Response		
Thank you for your response.		

Monika Montez	California Independent System Operator	Yes
Response		
Thank you for your response.		
Lana Smith	San Miguel Electric Cooperative, Inc.	No, The Draft Data Request feels like a trap. I do not see what usable data will come from this data request and I believe question # 6 about the costs proves that.
Response		
Thank you for your comment. Consistent with the May 2019 report *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions*, NERC believes that the data request will provide NERC with information that will enable it to better understand the potential supply chain risks associated with low impact BES Cyber Systems not presently subject to the Supply Chain Standards.		
William Kilfoyle	US Navy Kitsap	Yes
Response		
Thank you for your response.		
Sandra Revnell	Wolverine Power Supply Cooperative, Inc.	Yes
Response		
Thank you for your response.		
Masuncha Bussey	Duke Energy	No, Question #4 - 3.2, if a weighting will have to be completed, Duke Energy will need more time to answer the question. Also, Duke Energy purposes that question #4 be changed to read like this: "If you have medium or high impact BES Cyber Systems,

		please explain how your CIP-013-1 R1 plan will impact low BES Cyber Systems and any plans to apply to low assets in your plan:"
Response		
Thank you for your comment. NERC has revised Question #4.		
Roger Fradenburgh	Network & Security Technologies Inc.	Yes
Response		
Thank you for your response.		
Jonathan Robbins	Seminole Electric Cooperative, Inc.	
Response		
Thank you for your response.		
Wendy Center	U.S. Bureau of Reclamation	Yes
Response		
Thank you for your response.		
Wayne Sipperly	NAGF	Comments are incorporated in document emailed to H. Gugel on 7-18-19.
Response		
Thank you for your comment. NERC has reviewed the comments and incorporated changes as appropriate.		

Ming Nguyen	EDF Renewables	No
Response		
Thank you for your response.		
Joseph DePoorter	Madison Gas and Electric Company	No, No, not as currently written. Summary of comments. The proposed Data Request looks to review (count the locations of, etc.) All BES Cyber Systems, rather than just low impact BES Cyber Systems, which is the genesis of this Data Request. The data from this Data Request may be erroneous since Entities can organized their BES Cyber Systems in many different configurations (having many cyber assts in a BES Cyber System). We do not foresee how NERC can analyze the data on a simple count of systems. Please see our detailed comments address in question 5.
Response		
Thank you for your comment. NERC believes that information regarding all BES Cyber Systems is needed to evaluate relative risk.		
Scott Klauminzer	Tacoma Power	Yes
Response		
Thank you for your response.		
Vivian Moser	Arizona Public Service Co.	No
Response		
Thank you for your response.		

Mark Brown	City of Winter Park	Yes
Response		
Thank you for your response.		
Rodger Blakely	Santee Cooper	Yes
Response		
Thank you for your response.		
Davis Jelusich	Public Utility District No. 1 of Chelan County	Yes, CHPD agrees with the Supply Chain Data Request approach. It would be helpful to clarify how to handle an asset/location that has two distinct transmission assets that separately perform Medium and Low Impact BES functions, but happen to be co-located at the same location. For example, a Transmission station can have both a Medium Impact and a Low Impact BES Cyber System(s) within the same location/building, but are otherwise mutually exclusive of one another. Counting these two unique systems (1 at Medium, 1 at Low) makes sense, although the survey implies that the transmission station location should only be counted as Medium Impact and that the Low Impact system should be excluded. Consider revising the description for a "location". For example: "A 'location' includes any number of BES Cyber Systems at a given Asset, as defined in CIP-002-5.1a, that operate at a common Impact Rating."
Response		
Thank you for your comment. NERC has revised the text to address your comment.		

Bob Case	Black Hills Corporation	Yes, Much of the requested data should be able to come from entity's CIP-002 data in preparation for CIP-003-7. But I discovered that some DR questions regarding the details of remote connectivity go beyond what is captured in our current CIP-002 data and will have to be independently captured. It would be good to know in the DR narrative which questions are ad hoc, and which woud be considered data that entities should be aware of at all times.
Response		
Thank you for your comment. For this data request, entities should respond to all questions.		
Sean Bodkin	Dominion Energy	No, Dominion Energy agrees with the EEI comments and also believes the proposed questions may provide valuable data for NERC to begin assessing whether and how the supply chain risk management cyber security standard should apply to low impact BES Cyber Systems with external routable connectivity "erc." However, additional data will be needed and additional analysis performed with the expanded data to determine the risks these systems represent and the various options that will be needed to address or manage the identified risks.
Response		
Thank you for your comment. Please see response to EEI. Additional analysis may need to be performed in the future, but the scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested.		
David Rivera	New York Power Authority	No, The proposed data request appears to capture not only a complete 'Inventory' of every entities Low Impact assets, but also

		how they are being managed. This level of detail will require an 'extensive' amount of Subject Matter Expert time, since most of what is being asked for are not details which many (and probably most) entities would have a business need to gather and continuously update. A low impact cyber asset inventory is currently not required by CIP-002.
Response		
Thank you for your comment. 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.		
Veronica Murillo	Tucson Electric Power Company	No, The data request responses may provide some information to determine some indication of potential risks associated with the supply chain specifically in terms of the number of assets; however, there is no data around cost because we are still in the process of implementing CIP-013 for the High/Medium assets.
Response		
Thank you for your comment. NERC believes the comment is addressed through the inclusion of Question #7.		
Shonda McCain	OPPD	Yes, We have comments on the language used in the Data Request section of the draft. The paragraph that starts with "In NERC's 'Supply Chain..' report, NERC staff expects" at the bottom of page 5, we think it should not contain the word expects. This gives the impression that entities are 'expected' to 'voluntarily' include low impact assets. We understand that NERC predicts many utilities will do this, but this statement makes NERC's expectations unclear. Additionally, we would like to see language for low impact BES

		Cyber Systems with External Routable Connectivity added to this paragraph, similar to other statements in this draft.
Response		
Thank you for your comment. The referenced report uses the term “expects,” so it is included in that portion of the data request summarizing the report.		
Kevin Salsbury	NV Energy	No, NV Energy believes the proposed questions may provide valuable data for NERC to begin assessing whether and how the supply chain risk management cyber security standard should apply to low impact BES Cyber Systems with external routable connectivity ("erc"). However, additional data will be needed and additional analysis performed with the expanded data to determine the risks these systems represent and the various options that will be needed to address or manage the identified risks. Additional detail will be required, outside of location, such as: Patching capability, Authentication, Account management, vendor supported vs. legacy equipment, etc.
Response		
Thank you for your comment. NERC believes the requested data will provide NERC with the information it needs to begin developing a better understanding of the risks. Additional analysis may need to be performed in the future, but the scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested.		
Tho Tran	Oncor Electric Delivery	No, Oncor supports EEI's comment.
Response		

Thank you for your comment. Please see response to EEI.		
LaTroy Brumfield	American Transmission Company	No, ATC believes the proposed questions may provide valuable data for NERC to begin assessing whether and how the supply chain risk management cyber security standard should further consider low impact BES Cyber Systems with external routable connectivity "ERC". However, ATC also believes that considering the number of low impact sites w/ connectivity + risk score based on MW without consideration of supplier count may not provide NERC with a sufficient amount of data to address the directive for NERC to "study" the nature and "complexity" of cyber security supply chain risks, and develop recommendations for follow-up actions that will best address those risks. ATC suggests NERC broaden the scope of the data request to include a set of additional questions, that at a minimum will help NERC understand how many additional suppliers the expanded requirement(s) will bring into scope for Registered Entities.
Response		
Thank you for your comment. Based on the abbreviated time frame, NERC has declined to broaden the scope of this data request as suggested. Question #4 was modified to capture more information about suppliers of low impact BES Cyber Assets.		
Aaron Cavanaugh	Bonneville Power Administration	No, "Low Impact BCS with external routable connectivity" will not be received well by industry, this is a new concept, not a term of art, and is confusing when compared to ERC. BPA suggests changing this to "Low Impact BCS applicable to CIP-003-7 Attachment 1, Section 3".
Response		

Thank you for your comment. The data request has been revised.		
Davina Julienne	San Diego Gas & Electric	Yes, Low impact BES Cyber Systems should be included. Supply Chain Risk Assessment is too important to leave out a significant portion of the cyber population.
Response		
Thank you for your comment.		
Michael Johnson	Pacific Gas & Electric (PGAE)	Yes, PG&E agrees that the questions related to external connectivity are appropriate and helpful, but has the following input on the use of the phrase "external routable connectivity". The words "external routable connectivity", either capitalized or not capitalized is not used in CIP-003-7, Attachment 1, Section 3, which can result in confusion. PG&E recommends relying instead upon the actual wording in CIP-003-7 which is "necessary inbound and outbound electronic access as determined by the Responsible Entity" be used. If the text "external routable connectivity" is still desired by NERC, then PG&E recommends making "external routable connectivity" equivalent to the description appearing in the Attachment 1, Section 3 text. An example of this could be: "external routable connectivity" in this Data Request is meant to be the represent the same meaning as the CIP-003-7, Attachment 1, Section 3, Part 3.1 requirement language describing the function as "Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications …" and follow the CIP-003-7 Reference Models 1 through 10.
Response		

Thank you for your comment. The data request has been revised.		
Quintin Lee	Eversource	No, Additional information and analysis is needed to determine if the risks the low impact BES Cyber Systems with external routable should be considered.
Response		
Thank you for your comment. NERC believes that the data request will provide NERC with the additional information it needs to analyze these risks.		
Kent Feliks	American Electric Power Company Inc.	No, The data request should not be focused on numbers or types of assets. The collection of the data necessary to answer the questions in the data request would be extremely time consuming compared to a much simpler approach that AEP's suggests. As an alternative, AEP suggests determining if there are vendors that supply equipment used in Low Impact BES environments that are not also supplying systems for High and Medium Impact BES environments. This would identify the number of equipment venders that will not be covered under the current set of standards, and as such, if there are enough of these vendors to raise a reliability risk. (New Paragraph)The focus of the Supply Chain Standards, as currently written, is the supply chain and not the individual devices. (New Paragraph) Additionally, since Low Impact BES systems are excluded from many of the other CIP standards and are not required to be inventoried, so it would likely take an extraordinary amount of time to gather the information being requested.
Response		

Thank you for your comment. NERC believes that information regarding all BES Cyber Systems is needed to evaluate relative risk. In addition, Question #4 was modified to address your comment.		
Andrea Koch	EEI	No, EEI member companies believe the proposed questions may provide valuable data for NERC to begin assessing whether and how the supply chain risk management cyber security standard should apply to low impact BES Cyber Systems with external routable connectivity "erc." However, additional data and further analysis will be needed to determine the risks these systems represent and the various options that may be needed to address or manage identified risks.
Response		
Thank you for your comment. Additional analysis may need to be performed in the future, but the scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested.		
Michelle Longo	PPL Electric Utilities	Yes
Response		
Thank you for your response.		
Venona Greaff	Oxy	Yes
Response		
Thank you for your response.		

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.

Submitter Name	Submitter Company	Answer/Comment
Todd Candler	General Electric	Yes
Response		
Thank you for your response.		
Robert Gray	Board of Public Utilities (Kansas City KS) (BPU)	Yes
Response		
Thank you for your response.		
Kjersti Drott	Tri-State Generation and Transmission Assoc., Inc.	Yes
Response		
Thank you for your response.		
Monika Montez	California Independent System Operator	Yes
Response		

Thank you for your response.		
Lana Smith	San Miguel Electric Cooperative, Inc.	No, See # 1.
Response		
Thank you, please see response to #1.		
William Kilfoyle	US Navy Kitsap	Yes
Response		
Thank you for your response.		
Sandra Revnell	Wolverine Power Supply Cooperative, Inc.	Yes
Response		
Thank you for your response.		
Masuncha Bussey	Duke Energy	Yes, Duke Energy generally supports that these are the correct Reporting Entities for the Supply Chain Data Request.
Response		
Thank you for your response.		
Roger Fradenburgh	Network & Security Technologies Inc.	Yes
Response		
Thank you for your response.		

Jonathan Robbins	Seminole Electric Cooperative, Inc.	
Response		
Thank you for your response.		
Wendy Center	U.S. Bureau of Reclamation	Yes
Response		
Thank you for your response.		
Wayne Sipperly	NAGF	Yes
Response		
Thank you for your response.		
Ming Nguyen	EDF Renewables	Yes
Response		
Thank you for your response.		
Joseph DePoorter	Madison Gas and Electric Company	No, The proposed Data Request wants to know about all BES Cyber Systems, yet the purpose is to see how many low impact BES Cyber Systems are outside the applicability of the soon to be mandatory CIP-013-1 but are mitigating Supply Chain Management risks. Recommend that if NERC and the SCWG wants data for non-CIP-013-1 applicable Entities but must comply with CIP-002-5.1a, they should require data from low impact BES Cyber System owners, only. The intent of the Data Request should be if

		risks concerning supply chain management are being mitigated by low impact BES Cyber System owners. Entities have listened to the ERO's Enterprise Violation Themes webinar (CIP focused) and concur with NERC's Cyber Security Supply Chain Risks (within NERC's filing to FERC, RM17-13-000), it states, "NERC staff expects 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 outcome of the Data Request should be if low impact BES Cyber System are mitigating Supply Chain Management risks, not how many BES Cyber Systems there in applicable to CIP-002-5.1a.
Response		
Thank you for your comment. NERC believes that information regarding all BES Cyber Systems is needed to evaluate relative risk.		
Scott Klauminzer	Tacoma Power	Yes
Response		
Thank you for your response.		
Vivian Moser	Arizona Public Service Co.	Yes
Response		
Thank you for your response.		
Mark Brown	City of Winter Park	Yes
Response		

Thank you for your response.		
Rodger Blakely	Santee Cooper	Yes
Response		
Thank you for your response.		
Davis Jelusich	Public Utility District No. 1 of Chelan County	Yes
Response		
Thank you for your response.		
Bob Case	Black Hills Corporation	Yes
Response		
Thank you for your response.		
Sean Bodkin	Dominion Energy	Yes
Response		
Thank you for your response.		
David Rivera	New York Power Authority	Yes, That is probably the correct place to start, however there are probably other points of reference that should be used as well. For example, there are specific vendors that have a major impact on the controls required by all entities who use products and services from those vendors. These vendors should also be asked to provide similar (non-entity specific) information that they have

		gathered, which can paint a very clear picture of where the supply chain risks may either exist, or that are complicated by (or even aggravated) by those specific vendors. Although they are not ‘’obligated” to answer such questions from NERC, the industry should be made aware if key vendors they use are willing to assist their customers and clients through this evaluation and overall effort.
Response		
Thank you for your comment. Additional analysis may need to be performed in the future, but the scope of this data request was limited to allow registered entities to respond.		
Veronica Murillo	Tucson Electric Power Company	Yes
Response		
Thank you for your response.		
Shonda McCain	OPPD	Yes
Response		
Thank you for your response.		
Kevin Salsbury	NV Energy	Yes
Response		
Thank you for your response.		
Tho Tran	Oncor Electric Delivery	Yes, Oncor supports EEI's comment.

Response		
Thank you for your response.		
LaTroy Brumfield	American Transmission Company	Yes
Response		
Thank you for your response.		
Aaron Cavanaugh	Bonneville Power Administration	Yes, BPA agrees with the scope of the Supply Chain Risk Assessment Data Request.
Response		
Thank you for your response.		
Davina Julienne	San Diego Gas & Electric	Yes
Response		
Thank you for your response.		
Michael Johnson	Pacific Gas & Electric (PGAE)	Yes, PG&E provides no comments for this question.
Response		
Thank you for your response.		
Quintin Lee	Eversource	Yes
Response		

Thank you for your response.		
Kent Feliks	American Electric Power Company Inc.	Yes
Response		
Thank you for your response.		
Andrea Koch	EEI	Yes
Response		
Thank you for your response.		
Michelle Longo	PPL Electric Utilities	Yes
Response		
Thank you for your response.		
Venona Greaff	Oxy	Yes
Response		
Thank you for your response.		

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.

Submitter Name	Submitter Company	Answer/Comment
Todd Candler	General Electric	Yes
Response		
Thank you for your response.		
Robert Gray	Board of Public Utilities (Kansas City KS) (BPU)	Yes
Response		
Thank you for your response.		
Kjersti Drott	Tri-State Generation and Transmission Assoc., Inc.	Yes
Response		
Thank you for your response.		
Monika Montez	California Independent System Operator	Yes, We have 2 assets that contain BES Cyber Systems in the High classification; we do not have any low impact BCS.

Response		
Thank you for your response.		
Lana Smith	San Miguel Electric Cooperative, Inc.	No, See # 1.
Response		
Thank you for your comment. Please see response to #1.		
William Kilfoyle	US Navy Kitsap	The Navy IT policy group is blocking access to the WECC CDMS website and we are still trying to correct the blocked access., Yes
Response		
Thank you for your comment.		
Sandra Revnell	Wolverine Power Supply Cooperative, Inc.	No, Estimating the number of low impact BES Cyber systems, the number of those containing external routable connectivity, and the location risk score for low impact BES Cyber Systems will take time and expertise. While a one-time data request using, in part, the results analysis required under current CIP-002-5.1a, the estimated time to complete the data request will vary with the size of the entity; the fact that some entities may be currently engaged in a data submittal process for an audit engagement should be considered. 90 calendar days to respond to this, and future, data requests is a more universally reasonable timeframe.
Response		
Thank you for your comment. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Masuncha Bussey	Duke Energy	No, Duke Energy does not agree that the timeframe of 45 days is enought time to complete the data request. Recommendation, at least 6 months.
Response		
Thank you for your comment. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Roger Fradenburgh	Network & Security Technologies Inc.	
Response		
Jonathan Robbins	Seminole Electric Cooperative, Inc.	No, The response time period is dependent on NERC and FERC's clarifications to comments on the proposed Section 1600 Data Request.
Response		
Thank you for your comment. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		

Wendy Center	U.S. Bureau of Reclamation	No, Reclamation recommends extending the due date for the information from 45 days to 60 days to allow entities sufficient time to gather the required information and input from field SMEs, contracting offices, legal, and project management personnel. The longer response time will allow a greater quantity of more precise and accurate data to be collected.
Response		
Thank you for your comment. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Wayne Sipperly	NAGF	
Response		
Ming Nguyen	EDF Renewables	Yes
Response		
Thank you for your response.		
Joseph DePoorter	Madison Gas and Electric Company	No, Please note that this Data Request should be targeted to Entities who only have low impact BES Cyber Systems and not Entities that have low impact BES Cyber Systems. Regardless of categorization level of a BES Cyber System, Entities with low and either medium or high BES Cyber Systems will apply their supply

		chain cyber security risk management plan to all BES Cyber Assets that they have. If this Data Request is only directed to low impact BES Cyber System owners, they may not have the talent or expertise to accomplish the requested Data Request within 45 days.
Response		
Thank you for your comment. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Scott Klauminzer	Tacoma Power	Yes
Response		
Vivian Moser	Arizona Public Service Co.	No
Response		
Thank you for your response.		
Mark Brown	City of Winter Park	Yes
Response		
Thank you for your response.		
Rodger Blakely	Santee Cooper	Yes

Response		
Thank you for your response.		
Davis Jelusich	Public Utility District No. 1 of Chelan County	Yes
Response		
Thank you for your response.		
Bob Case	Black Hills Corporation	Yes, 45 days to respond is appropriate after 01-Jan-2020 (effectivity date of CIP-003-7). If the DR is issued prior to 01-Jan-2020, entities should still be given until mid-Feb 2020 to respond. Prudent entities will have a good handle on most of their Low Impact data well in advance of 01-Jan-2020, but it will likely still be a mad dash to clear up last minute discoveries leading to the CIP-003-7 effectivity date. For the most accurate data, which will be the most benefit to NERC, DR submission should be deferred until after 01-Jan-2020.
Response		
Thank you for your comment. Entities are required to respond in 2019. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Sean Bodkin	Dominion Energy	No, InDominion Energy supports EEI comments and agrees that in order for the NERC Board of Trustees to make decision on this issue that has a positive impact on reliability, EEI requests that NERC consider the fact that most entities are currently working to

		ensure compliance with CIP-003-7 by January 1, 2020. The preparations for CIP-003-7 have a direct impact on the resources available for the proposed Section 1600 data request as well as on the accuracy of the data on low impact BES Cyber Systems. NERC may only receive best estimates (e.g., question 4 criterion 3.2, questions 5.d. through 5.g.) that are incomplete if the proposed Section 1600 data request is made prior to the implementation date of CIP-003-7.
Response		
Thank you for your comment. NERC clarifies that it is seeking estimated information regarding low impact BES Cyber Assets and has made revisions to this effect in the data request. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
David Rivera	New York Power Authority	Yes, Having to respond in such a limited time-frame would present an enormous lift for our organization due to its level of required detail. Although we could defer all existing CIP compliance efforts, which would pull resources away from other critical projects that have a direct impact on our ability to complete the work on implementing the current CIP-013 requirements (and scope). Also, some of the resources we would need are engaged in critical operational roles, and having them leave their post to answer all these details could impact the reliability of the BES assets we are operating.
Response		

Thank you for your comment. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Veronica Murillo	Tucson Electric Power Company	No, It will be a significant effort to compile the responses to the data request and will involve many of the same resources already working on the implementation of the CIP-003-7. The timing of the data request will jeopardize our ability to meet the January 1, 2020 compliance deadline.
Response		
Thank you for your comment. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Shonda McCain	OPPD	Yes
Response		
Thank you for your response.		
Kevin Salsbury	NV Energy	No, In order for the NERC BOT to make a decision on this issue that has a positive, and significant, impact on reliability, NV Energy requests that NERC consider the fact that most entities (especially entities with a large number of low impact facilities) are currently working to ensure compliance with CIP-003-7 by January 1, 2020. The preparations for CIP-003-7 have a direct impact on the available resources for the completion of the proposed Section

		1600 data request, and as such, the accuracy of the data on low impact BES Cyber Systems. NERC may only receive best estimates (e.g., question 4 criterion 3.2, questions 5.d. through 5.g.) that may be incomplete if the proposed Section 1600 data request is made prior to the implementation date of CIP-003-7. Given the CIP Standards (CIP-002-5.1a) are written that an entity is not required to inventory their low impact BES cyber systems, there will be entities that will require a significant amount of resources and manhours to inventory thier systems, especially if the entity has a significant amount of low impact facilities. NV Energy recommends the Data Request be issued after the implementation date of CIP-003-7, and the timeframe for completion be extended to at a minimum of 90 days.
Response		
Thank you for your comment. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Tho Tran	Oncor Electric Delivery	No, Oncor supports EEI's comment.
Response		
Thank you for your comment. Please see response to EEI.		
LaTroy Brumfield	American Transmission Company	No, ATC endorses the comments of EEI n this matter
Response		

Thank you for your comment. Please see response to EEI.		
Aaron Cavanaugh	Bonneville Power Administration	Yes, BPA can respond to the proposed data request within the specified timeframe.
Response		
Thank you for your response.		
Davina Julienne	San Diego Gas & Electric	Yes, A short time frame may risk the quality of the data.
Response		
Thank you for your response.		
Michael Johnson	Pacific Gas & Electric (PGAE)	Yes, PG&E believes the 45-day due date should provide sufficient time to complete the data request.
Response		
Thank you for your response.		
Quintin Lee	Eversource	Yes, We agree with the 45 day due date for the draft data request.
Response		
Thank you for your response.		
Kent Feliks	American Electric Power Company Inc.	No, As mentioned in our response to question #1, most Low Impact BES system are not subject to CIP requirements, and as such, are not currently inventoried. Thus, it will take a substantial amount of time (months, if not years) to perform an accurate

		inventory, as there are tens of thousands of these systems across just AEP's system, let alone across the entire nation. Additionally, answering this request at this time could cause delay in compliance with this standard and others in progress by taking attention away from them to answer this request.
Response		
Thank you for your comment. NERC clarifies that it is seeking estimated information regarding low impact BES Cyber Assets, rather than a complete inventory, and has made revisions to this effect in the data request.		
Andrea Koch	EEI	No, For the NERC Board of Trustees to make a decision on this issue that has a positive impact on reliability, EEI requests that NERC consider the fact that most entities are currently working to ensure compliance with CIP-003-7 by January 1, 2020. The preparations for CIP-003-7 have a direct impact on the resources available for the proposed Section 1600 data request as well as on the accuracy of the data on low impact BES Cyber Systems. NERC may only receive imprecise estimates (e.g., question 4 criterion 3.2, questions 5.d. through 5.g.) if the proposed Section 1600 data request is made prior to the implementation date of CIP-003-7.
Response		
Thank you for your comment. NERC clarifies that it is seeking estimated information regarding low impact BES Cyber Assets and has made revisions to this effect in the data request. The scope of this data request was limited to allow entities to respond to the questions and NERC staff to analyze the data and provide results to the NERC Board in November, as requested. 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.		
Michelle Longo	PPL Electric Utilities	Yes

Response		
Thank you for your response.		
Venona Greaff	Oxy	Yes
Response		
Thank you for your response.		

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.

Submitter Name	Submitter Company	Answer/Comment
Todd Candler	General Electric	No, The data request is asking for the number of specific types of connectivity. As a Low Impact entity we don't maintain an inventory of individual pieces of equipment.
Response		
Thank you for your comment.		
Robert Gray	Board of Public Utilities (Kansas City KS) (BPU)	Yes
Response		
Thank you for your response.		
Kjersti Drott	Tri-State Generation and Transmission Assoc., Inc.	Yes
Response		
Thank you for your response.		

Monika Montez	California Independent System Operator	Yes, We don't have low impact BES Cyber Systems.
Response		
Thank you for your response.		
Lana Smith	San Miguel Electric Cooperative, Inc.	No, See # 1.
Response		
Thank you for your comment. Please see response to #1.		
William Kilfoyle	US Navy Kitsap	Yes
Response		
Thank you for your response.		
Sandra Revnell	Wolverine Power Supply Cooperative, Inc.	Yes
Response		
Thank you for your response.		
Masuncha Bussey	Duke Energy	No comment.
Response		
Thank you.		
Roger Fradenburgh	Network & Security Technologies Inc.	Yes

Response		
Thank you for your response.		
Jonathan Robbins	Seminole Electric Cooperative, Inc.	No, In the proposed response to the data request posted by the drafting team, the response on page 11 appears to include the specific sites that are participating in certain programs, such as the Neighborhood Keeper program. This information may merely be listed for informational purposes to help entities complete the following table, however, Seminole wishes to confirm this reasoning with the draft team. Seminole has concern that by identifying which sites are participating, an entity is also indicating which sites are not participating, and this disclosure could be considered sensitive information. If Seminole is merely required to complete the table, that may not be issue except that it still may not be wise to indicate how many locations of each entity are participating in an industry security program.
Response		
Thank you for your comment. NERC clarifies that no identification of any location is being requested.		
Wendy Center	U.S. Bureau of Reclamation	Yes
Response		
Thank you for your comment.		
Wayne Sipperly	NAGF	Yes
Response		

Thank you for your response.		
Ming Nguyen	EDF Renewables	No
Response		
Thank you for your response.		
Joseph DePoorter	Madison Gas and Electric Company	Yes, None.
Response		
Thank you for your response.		
Scott Klauminzer	Tacoma Power	Yes
Response		
Thank you for your response.		
Vivian Moser	Arizona Public Service Co.	No
Response		
Thank you for your response.		
Mark Brown	City of Winter Park	Yes
Response		
Thank you for your response.		

Rodger Blakely	Santee Cooper	Yes
Response		
Thank you for your response.		
Davis Jelusich	Public Utility District No. 1 of Chelan County	Yes
Response		
Thank you for your response.		
Bob Case	Black Hills Corporation	Yes, Although the data requested has been carefully selected to avoid conflict with Section 1501 of the NERC RoP, the information requested in aggregate is still considered very descriptive of cyber threat vectors across the grid. My concern is the perception that all of industry's attributable responses will be in one repository. If that one storage location is, or has been compromised, I would be worried about the long-term potential consequences. To that end, some words of assurance in the DR may increase entity confidence and improve the completeness of DR submissions.
Response		
Thank you for your response. NERC intends to release the information publicly in summary/aggregate form only.		
Sean Bodkin	Dominion Energy	No, Dominion Energy supports EEi comments and agrees that the requested information may be considered Confidential Information if it is not aggregated or provides the identity of the entity. The number of low impact facilities combined with the security attributes requested in question 5.d. through 5.g. could be

		useful to an adversary seeking to disrupt the BES. EEI recommends that NERC only provide anonymous and aggregated data to FERC or other government entities or seek to protect this information from public disclosure.
Response		
Thank you for your comment. Please see response to EEI.		
David Rivera	New York Power Authority	No, Although we do not consider such information as Cyber System Information (CSI), our corporate information protection program would consider such details as business confidential.
Response		
Thank you for your comment. NERC does not believe the requested information meets the definition of Confidential Information as it is defined in Section 1500 of the NERC Rules of Procedure.		
Veronica Murillo	Tucson Electric Power Company	No, The data request is seeking non-public information, and if the data is not aggregated so that individual utilities are not identified, the information may potentially be CEII. The number of low impact facilities combined with the security attributes requested in question 5.d. through 5.g. could be useful to an adversary seeking to disrupt the BES.
Response		
Thank you for your comment. NERC does not believe the requested information meets the definition of Confidential Information as it is defined in Section 1500 of the NERC Rules of Procedure. NERC, however, will publicly release the data in summary/aggregate form only. Individual responses will not be made public.		

Shonda McCain	OPPD	Yes
Response		
Thank you for your response.		
Kevin Salsbury	NV Energy	No, The requested information may be considered Confidential Information if it is not aggregated or provides the identity of an entity. The number of low impact facilities combined with the security attributes requested in question 5.d. through 5.g. could be useful to an adversary seeking to disrupt the BES. NV Energy shares EEI's recommendation that NERC only provide anonymous and aggregated data to FERC or other government entities or seek to protect this information from public disclosure.
Response		
Thank you for your comment. NERC does not believe the requested information meets the definition of Confidential Information as it is defined in Section 1500 of the NERC Rules of Procedure. NERC, however, will publicly release the data in summary/aggregate form only. Individual responses will not be made public.		
Tho Tran	Oncor Electric Delivery	No, Oncor supports EEI's comment.
Response		
Thank you for your comment. Please see response to EEI.		
LaTroy Brumfield	American Transmission Company	No, ATC endorses the comments of EEI n this matter
Response		

Thank you for your comment. Please see response to EEI.		
Aaron Cavanaugh	Bonneville Power Administration	No, BPA is always concerned about CEII and will follow the guidance from page 9, section "Restrictions on disseminating data (Confidential/CEII.)" In addition, Freedom of Information Act (FOIA) exemptions may apply in some cases. NERC is not requesting specific information relative to BES Cyber Systems that would create the need to invoke critical energy infrastructure confidentiality provisions. 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.
Response		
Thank you for your comment.		
Davina Julienne	San Diego Gas & Electric	Yes
Response		
Thank you for your response.		
Michael Johnson	Pacific Gas & Electric (PGAE)	Yes, PG&E does not believe that the requested information, when combined with other Entity data, will contain Confidential Information.
Response		
Thank you for your response.		

Quintin Lee	Eversource	No, The requested information may be considered Confidential Information if it is not aggregated or provides the identity of the entity. The number of low impact facilities combined with the security attributes requested in question 5.d. through 5.g. could be useful to an adversary seeking to disrupt the BES. Everssource recommends that NERC only provide anonymous and aggregated data to FERC or other government entities or seek to protect this information from public disclosure.
Response		
Thank you for your comment. NERC does not believe the requested information meets the definition of Confidential Information as it is defined in Section 1500 of the NERC Rules of Procedure. NERC, however, will publicly release the data in summary/aggregate form only. Individual responses will not be made public.		
Kent Feliks	American Electric Power Company Inc.	No, AEP feels that that the data being requested should be considered Critical Energy Infrastructure Information as included in the definition of Confidential Information in Section 1501 of the NERC Rules of Procedure.
Response		
Thank you. NERC does not agree that the requested information meets the definition of Confidential Information as it is defined in Section 1500 of the NERC Rules of Procedure.		
Andrea Koch	EEI	No, The requested information may be considered Confidential Information if it is not aggregated or provides the identity of the entity. The number of low impact facilities combined with the security attributes requested in question 5.d. through 5.g. could be useful to an adversary seeking to disrupt the BES. EEI recommends that NERC only provide anonymous and aggregated data to FERC

		or other government entities. In addition, NERC should protect this information from public disclosure by ensuring a secure mode of submission.
Response		
Thank you for your comment. NERC does not believe the requested information meets the definition of Confidential Information as it is defined in Section 1500 of the NERC Rules of Procedure. NERC, however, will publicly release the data in summary/aggregate form only. Individual responses will not be made public.		
Michelle Longo	PPL Electric Utilities	Yes
Response		
Thank you for your response.		
Venona Greaff	Oxy	Yes
Response		
Thank you for your response.		

5. Provide any additional comments for NERC staff and the SCWG to consider, if desired.		
Submitter Name	**Submitter Company**	**Answer/Comment**
Todd Candler	General Electric	Isn't clear to me how this provides information on the way an entity deals with its vendors.
Response		
Thank you for your comment. The purpose of this data request is to enable NERC to obtain information that will enable it to better understand the supply chain risks associated with low impact BES Cyber Systems that are not presently subject to the Supply Chain Standards.		
Masuncha Bussey	Duke Energy	Question # 5 (Impact Categorization BES Cyber Systems)Duke Energy requests that more clarification is needed for partsD-(Number of locations allowing third party remote access to a BES CyberSystem), and E-(Number of locations with third party monitoring of the asset toa BES Cyber System).
Response		
Thank you for your comment. Access and monitoring have been clarified in the footnotes.		
Roger Fradenburgh	Network & Security Technologies Inc.	The section, "CIP-013 Cost of Implementation" states, "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." N&ST suggests adding appropriate attributions.The section, "CIP-013 Cost of Implementation" notes that the costs

		associated with replacing "blacklisted vendors" may be significant. N&ST suggests identifying the source(s) of information about such blacklisted vendors (we presume it is the 2019 National Defense Authorization Act).
Response		
Thank you for your comment. NERC feels that the language is clear as it stands and has made no change in response.		
Jonathan Robbins	Seminole Electric Cooperative, Inc.	Under Question 3, there is a chart. The chart indicates an entry for “low impact” and another entry for “low impact with erc”. Is the entry for “low impact” inclusive of the number listed in the “low impact with erc”?In the provided response to Question 4, the response appears to be vague: “HVP plans on applying CIP-013-1 controls” and Seminole wishes to confirm this is the intent of the drafting team.Regarding Question 6, Seminole recommends deleting this question and the associated comments as these questions and responses should have been submitted to FERC already as part of the CIP-013 project during the drafting phase.Regarding Question 5, F states “Number of locations with constant monitoring of remote connectivity to a BES Cyber System”. What does constant monitoring mean? Can entities be provided with examples?
Response		
Thank you for your comment. The language was modified to clarify that low impact is inclusive of low impact with external connectivity. As regarding costs, the question was included in response to comments received during development of the Supply Chain report. A footnote was added to clarify what is meant by constant monitoring.		

Wendy Center	U.S. Bureau of Reclamation	Reclamation recommends revising the Supply Chain Data Request to clarify and align terms used in the data request (e.g., “location,” “physical space,” “asset,” “risk,” and “mitigation”) with terms used in current enforceable CIP standards, and address inconsistencies between the definitions in the data request and the definitions contained in the NERC Glossary of Terms; specifically, External Routable Connectivity, BES Cyber Systems, BES Cyber Assets.
Response		
Thank you for your comment. The terms were reviewed throughout the document and modifications were made where appropriate.		
Wayne Sipperly	NAGF	See document emailed to H. Gugel on 7-18-19 for NAGF comments.
Response		
Thank you for your comments. NERC has reviewed the comments and incorporated changes as appropriate.		
Joseph DePoorter	Madison Gas and Electric Company	1. The Preface, Introduction, and Authority all correct. 2. Page 3, “How the data will be used” clearly states that the outcome of the data request may be used to justify that low impact BES Cyber Systems are included into CIP-013, Supply Chain Management. The proposed Data Request asks mainly for numbers of BES Cyber Systems. The intent of the Data Request should be is Supply Chain Management risk of low impact BES Cyber Systems being mitigated? 3. Page 3, How the data will be collected and validated paragraph, it states, “NERC will identify the registered entities necessary to complete the survey”. We do not know if this implies every

		Registered Entity or a random sample of Registered Entities? This does not line up with question 2 on the comment form which states, "2. The Reporting Entities for the Supply Chain Data Request are all registered entities that are required to comply with CIP-002-5.1a". Please clarify. 4. Page 5, second to last paragraph it states, "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 comment form and survey do not ask anything else about our internal programs that mitigate our supply chain management risks outside the scope of applicable CIP-013-1 Entities. If NERC Staff expects low impact BES Cyber System owners to have risk mitigating processes in place, why have a physical count of assets? The intent of the Data Request is based on NERC's filling to FERC RM-17-13-000. 5. Page 6, chart on top of page. Not sure why "Low impact" and "Low impact with erc" are both listed? If a BES asset did not have an external routable connectivity, it should not be classified as a low impact BES Cyber System. Please clarify. We also question the number of BES Cyber Systems that NERC will receive in this Data Request. CIP-002-5.1a (page 4 of 37) allow Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. This means that the data NERC receives is not a single set of data points, just a number of BES Cyber Systems which may contain one of many cyber assets. Without NERC

		knowing every Entity's process to determine if they have BES Cyber Systems or not, NERC cannot quantify how many BES Cyber Systems there are. 6. Page 6, Location Risk Score Table. It states, "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". There are no Location Risk Score of 1 list for an Entity to choose. Please clarify. If an Entity does not own or operate a Criterion, would that score be 0 (zero)? This needs to be clearly stated and shown in an example. 7. Page 6, Location Risk Score Table, Criterion 3.1, Risk Criterion column, what is meant by "MW Controlled"? Is this based on an all-time hourly peak load for a BA? Is this the amount of generation that a GOP directly operates? Note a GOP only operates a generator, the BA controls the output of MWs for each generator in their portfolio based on system flows, ACE, N-1 conditions, economics, etc. There may be multiple GOPs within a BA area, as well. Recommend that GOP be removed from foot note 5 since it should be captured under Criterion 3.3. 8. Page 7 part 5, Impact Categorization BES Cyber System table. Under Column 3.1, if an Entity has a low impact BES Cyber System with an erc, would that only be counted as 1 on line "b" Please clarify? Please clarify Line "f" the word "monitoring"? Is this physical, electronic or some other type of monitoring? Line "g". Is NERC implying that if a low impact BES Cyber System is part an industry program, that then mitigates our Cyber risks? Please clarify. Line "h". We do not understand why a listing of locations would be needed by NERC that have BES Cyber Systems that fall outside what is applicable to CIP-002-5.1a and hence require controls under the current version of CIP-003? Recommend that line 'h" be deleted. 9. Page 9, Example Response. CIP-013-1 is applicable

		to High and Medium BES Cyber Systems and requires the development of supply chain cyber security risk management plans. In Chapter 4 of NERC's Cyber Security Supply Chain Risks (within NERC's filing to FERC, RM17-13-000), it states, "As a best practice, NERC staff expects entities that have medium or high impact BES Cyber Systems will voluntarily apply CIP-013-1 Requirement R1 supply chain risk management plans to low impact BES Cyber Systems. This would help reduce the residual risks arising from the supply chain to those systems. Any cyber asset types identified as exclusive to low impact BES Cyber Systems should be evaluated on a case-by-case basis to determine the impact and extent of any supply chain risk management risks, which, if realized, could present a significant threat to the reliability of the BES. For entities that own both low and medium or high impact BES Cyber Systems, applying such practices to all assets regardless of destination would not only reduce the risks to its low impact BES Cyber Systems, but would also help streamline procurement and deployment processes generally". Does NERC believe that an Entity that has either a High or Medium BES Cyber System would not apply the same (required) supply chain cyber security risk management plans to their low impact BES Cyber Systems? We believe that the applicable Entities to CIP-013-1 will apply their "plans" to all BES Cyber Assets regardless of their categorization. If this data request is designed to capture BES Cyber Systems that CIP-013-1 is not applicable to, then there should be an example which ONLY contains low impact BES Cyber Systems.
Response		

Thank you for your comment. Several of the questions, footnotes, and instructions were modified to address the stated concerns.		
Scott Klauminzer	Tacoma Power	Question 4 implies that there is a compliance burden in CIP-013 for low-impact BES Cyber Systems.Question 4: "If you have medium or high impact BES Cyber Systems, please explain your plans to apply CIP-013-1 R1 to your low impact BES Cyber Systems:",
Response		
Thank you for your comment. Such an approach is not mandated by the standard, but was recommended in the May 2019 report *Supply Chain Risks: Staff Report and Recommended Actions.*		
Vivian Moser	Arizona Public Service Co.	Comments for Question 1: The proposed Supply Chain Data Request focuses extensively on the number of low impact BES Cyber Systems with external routable connectivity and locations containing these systems, but little on the procurement mechanisms, methodologies, and processes associated with the procurement of these and other applicable assets. Thus, the data proposed to be collected will not be indicative of a Reporting Entity's supply chain strategy and whether it is sufficiently expansive to address the procurement risks related to low impact systems. As most entity's engage in a consolidated or holistic procurement strategy, information regarding such processes would provide greater insight into costs, burden, and impact. Further, information related to quantity and risk scores could be beneficial in the appropriate context; however, its collection when undefined, unweighted, and not able to compared to or utilized within similar scoring systems for other applicable assets will reduce the applicability of that data to the identification and valuation of benefits. In

		summary, shifting the focus of the data request to information related to a Reporting Entity's CIP-013 procurement processes and strategies would be more effective at highlighting the burden, benefits, and costs associated with the addition of low impact assets to the applicability for CIP-013. Comments for Question 3: The identification of low impact BES Cyber Systems with external routable connectivity (ERC) is not required by the CIP standards, thus making collection of this information an entirely new endeavor, which is onerous and unduly burdensome given the assessment being conducted. Producing this information would divert critical resources currently dedicated to implementing CIP-003-7 by the January 1, 2020 effective date. Given the quantity of low impact BES Cyber Systems requiring evaluation to produce the requested information ERC information, AZPS proposes a minimum of 180 days to complete the data request. Comments for Question 4: The type of data being requested may not rise to the level of BES Cyber System Information (BCSI) or Critical Energy Infrastructure Information (CEII) but does contain a certain level of sensitivity for the Reporting Entity. For example, data and information can be linked to entities, which can be linked to physical locations, which can then be linked to systems of impact. To ensure the security of entity locations and systems, AZPS recommends that any entity-specific information or information that could be logically traced back to a specific entity should not be made publicly available, e.g., should be considered confidential.
Response		
Thank you for your comments. NERC responds as follows:		

#1: Additional analysis may need to be performed in the future, but the scope of this data request was limited to allow NERC staff to report to the NERC Board in November, as requested. #3: NERC is seeking estimated information, not a complete inventory. #4: NERC does not intend to publicly release individual entity responses. Collected information will be publicly reported in summary/aggregate form only.		
Bob Case	Black Hills Corporation	The inclusion of a sample submittal in the DR was a good move. Doing so was an acknowledgement by NERC that interpretations across the ERO regions on these matters vary. And the sample itself is an excellent tutorial. When submitting this comment form at 8:40am MT on Jul 22nd, submittal would not complete, and I received a notice of server error. Luckily, I was able to manually capture all my inputs for a later attempt to submit. However, many entities may get frustrated and abort their attempt to provide comments. It would be much appreciated if submitters were able to save a full copy of their Comments response (this applies to all NERC comment forms). Unless comments are expected to be limited to 28 characters, the field for comment submission are recommended to be wider, and multi-line. Thanks.
Response		
Thank you for your comments.		
Sean Bodkin	Dominion Energy	Dominion Energy supports EEI comments and agrees upon the EEI recommendation that a number of clarifications that may help NERC receive more consistent results from Registered Entities. First, it would be helpful to further clarify whether a generation resource with multiple units (not segmented) is

		considered one location and whether a generation resource with multiple segmented generation units is considered one or multiple locations. Second, we recommend that NERC clarify the meaning of the third-party remote access in question 5.d. (e.g., is a data diode considered remote access). Third, the term "constant monitoring" in question 5.f. is unclear. Fourth, we recommend that NERC consider updating the language in 5.g. to "Number of locations participating in gov/industry cybersecurity programs" as well as revising footnote 10 to Government/Industry cybersecurity programs such as CRISP, CYOTE, Neighborhood Keeper, etc. prior to requesting the data. And finally, we recommend that NERC clarify that if a company participates in CRISP at the corporate level, does that mean all or none of its locations are covered in response to question 5.g?
Response		
Thank you for your comments. Please see response to EEI.		
David Rivera	New York Power Authority	The timing of this data request has potential to impact the on-going CIP-013 preparation efforts. Also, what happened to question #5? Did we somehow go into the wrong system to provide these comments?
Response		
Thank you for your comments.		
Veronica Murillo	Tucson Electric Power Company	1. Can the data request wait to be issued after January 1, 2020? Following the CIP-003-7 implementation, the entity

		should have the requested information ready and the resources available to respond to the data request. Additionally, the entity will have the applicable protections in place. 2. Is there an alternative approach to determine the risk?
Response		
Thank you for your comment. NERC is moving with all deliberate speed to obtain the information it needs to evaluate supply chain risks associated with low impact BES Cyber Systems.		
Shonda McCain	OPPD	Please see our comments under question 1 regarding language in the Data Request Draft and repeated below: We have comments on the language used in the Data Request section of the draft. The paragraph that starts with "In NERC's 'Supply Chain..' report, NERC staff expects" at the bottom of page 5, we think it should not contain the word expects. This gives the impression that entities are 'expected' to 'voluntarily' include low impact assets. We understand that NERC predicts many utilities will do this, but this statement makes NERC's expectations unclear. Additionally, we would like to see language for low impact BES Cyber Systems with External Routable Connectivity added to this paragraph, similar to other statements in this draft.
Response		
Thank you for your comment. Please see response under Question #1.		
Kevin Salsbury	NV Energy	NV Energy requests a number of clarifications that may help NERC receive more consistent results from NV Energy and

		other Registered Entities. First, it would be helpful to further clarify whether a generation resource with multiple units (not segmented) is considered one location and whether a generation resource with multiple segmented generation units is considered one or multiple locations. Second, we recommend that NERC clarify the meaning of the third-party remote access in question 5.d. (e.g., is a data diode considered remote access). Third, the term "constant monitoring" in question 5.f. is unclear. Fourth, NV Energy recommends that NERC consider updating the language in 5.g. to "Number of locations participating in gov/industry cybersecurity programs" as well as revising footnote 10 to Government/Industry cybersecurity programs such as CRISP, CYOTE, Neighborhood Keeper, etc. prior to requesting the data. And finally, we recommend that NERC clarify that if a company participates in CRISP at the corporate level, does that mean all or none of its locations are covered in response to question 5.g?
Response		
Thank you for your comment. The terms access and monitoring were further clarified. In addition, clarification around the government/industry programs was addressed. Additionally, the following language was added: 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.		
LaTroy Brumfield	American Transmission Company	ATC endorses the comments of EEI n this matter.
Response		
Thank you for your comment. Please see response to EEI.		

Davina Julienne	San Diego Gas & Electric	The more the DR is rushed the greater the risk to having to a redo later.
Response		
Thank you for your comment. NERC is moving with all deliberate speed to obtain the information it needs to evaluate supply chain risks associated with low impact BES Cyber Systems.		
Michael Johnson	Pacific Gas & Electric (PGAE)	1 - As noted in Question 1 of the Comment form, the text of "external routable connectivity", either capitalized or not capitalized is not used in CIP-003-7, Attachment 1, Section 3 and could result in Entity confusion. PG& E recommends this be corrected using the information provided in Question 1. 2 – If the text of "external routable connectivity" is preferred, or if it is replaced with alternative language, its first use on page 3 in the section titled "How the data will be used" should contain the necessary footnote on any clarification information or a more refined definition of the intended meaning. PG& E recommends the initial footnote (FN4) covering this text on page 6 be moved here since this is its first use of the language and could help immediately set up how it is being used. All other references to this language or its replacement should then point back to the original reference on page 3. 3 - Starting on page 5 are the questions NERC is requesting data on. The first section is titled "General Questions:", but the section below that titled "BES Cyber Systems" which contains questions 2, 4 and 5 do not have the colon (:) like the other sections. Recommend this be corrected for consistency. 4 - The four (4) paragraphs right after the question title of "BES Cyber Systems" appear to set up what is needed in Question 3 on page 5, but that is not clear and took

		several readings to make this conclusion. PG& E recommends text be added before the first paragraph to indicate the information which follows are for Question 3. The same ambiguous condition occurs on page 6, right after Question 4. On initial reading, it appears the text which follows Question 4 are for that question. After several readings, however, it became apparent it was not. Rather, it was for the table and Question 5, which follows the paragraph. PG& E recommends clarifying that the paragraph and table are to help provide the information for Question 5. 5 - PG& E understands the use of word "location" which starts on PDF page 10 but is concerned it will result in potential over counting of some BES Cyber System (BCS) types. One example of this unexpected consequence would be for Transmission substation or station (3.2) which could also contain SPS/RAS (3.5). The paragraph before the table starting on PDF page 11 indicates this should not occur, but it is not clear on initial reading. PG& E recommends that the following existing draft language: "For each location, use the first criterion that applies (i.e., count each location once) …" Be changed to: "For each location containing different or multiple assets, use the first criterion that applies (i.e., count each location only once) …" Also, PG& E suggests placing a footnote after this paragraph to reference the Example Response section starting on PDF page 14. This will help the reader find answers to their questions early and avoid confusion. 6 - Footnote #6 on PDF page 11 is to avoid double counting generation resources in Question 5 which have been segmented into low impact BCS, as medium impact BCS in Question 4. PG& E recommends this footnote be first

		shown in Question 4 and then referenced again in Question 5 to highlight earlier the potential of double counting.
Response		
Thank you for your comments. NERC's responses are as follows: 1. Please see response to Question #1 2. The term "external routable connectivity" was replaced throughout the document to avoid confusion. 3. Corrected. 4. Changes made to address the concern. 5. Language was clarified to address the concern. 6. Language was changed to address the concern.		
Kent Feliks	American Electric Power Company Inc.	As previously stated, this data request is focused on the assets themselves and not the vendors who supply the assets (the supply chain). AEP feels that NERC should be focusing on collecting data on the vendors and ensuring the entities are evaluating those vendors for the production and distribution of reliable and secure equipment. This approach would be much less time consuming, while still providing the full value sought in this data collection effort.
Response		
Thank you for your comments. Please see response to previous comments.		
Andrea Koch	EEI	EEI recommends several clarifications that may help NERC receive more consistent results from Registered Entities. First, we recommend that NERC clarify the meaning of the third-party remote access in question 5.d. (e.g., is a data diode considered remote access). Second, the term "constant

		monitoring" in question 5.f. is unclear. Third, EEI recommends that NERC consider updating the language in 5.g. to "Number of locations participating in gov/industry cybersecurity programs" as well as revising footnote 10 to Government/Industry cybersecurity programs such as CRISP, CYOTE, Neighborhood Keeper, etc. prior to requesting the data. Fourth, we recommend that NERC clarify that if a company participates in CRISP at the corporate level, does that mean all or none of its locations are covered in response to question 5.g? And finally, it would be helpful to further clarify whether a generation resource with multiple units (not segmented) is considered one location and whether a generation resource with multiple segmented generation units is considered one or multiple locations.
Response		
Thank you for your comments. The terms access and monitoring were further clarified. In addition, clarification around the government/industry programs was addressed. Additionally, the following language was added: 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.		
Michelle Longo	PPL Electric Utilities	Question 4 should have 4 options for the responses: Are you doing the same for Lows as for High/Medium. Not yet decided Lows are excluded from program Other – Explain. Move paragraph starting wit "In order to help NERC ..." and the associate location risk score table to be part of Question 5 for clarity. As currently formatted it appears to be part of question 4.

Response
Thank you for your comments. Clarity was added to question #4, and a heading was added to show the break between question 4 and 5.

End of Report