NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Risk Assessment

Analysis of Data Collected under the NERC Rules of Procedure Section 1600 Data Request

December 9, 2019

RELIABILITY | RESILIENCE | SECURITY




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

Table of Contents

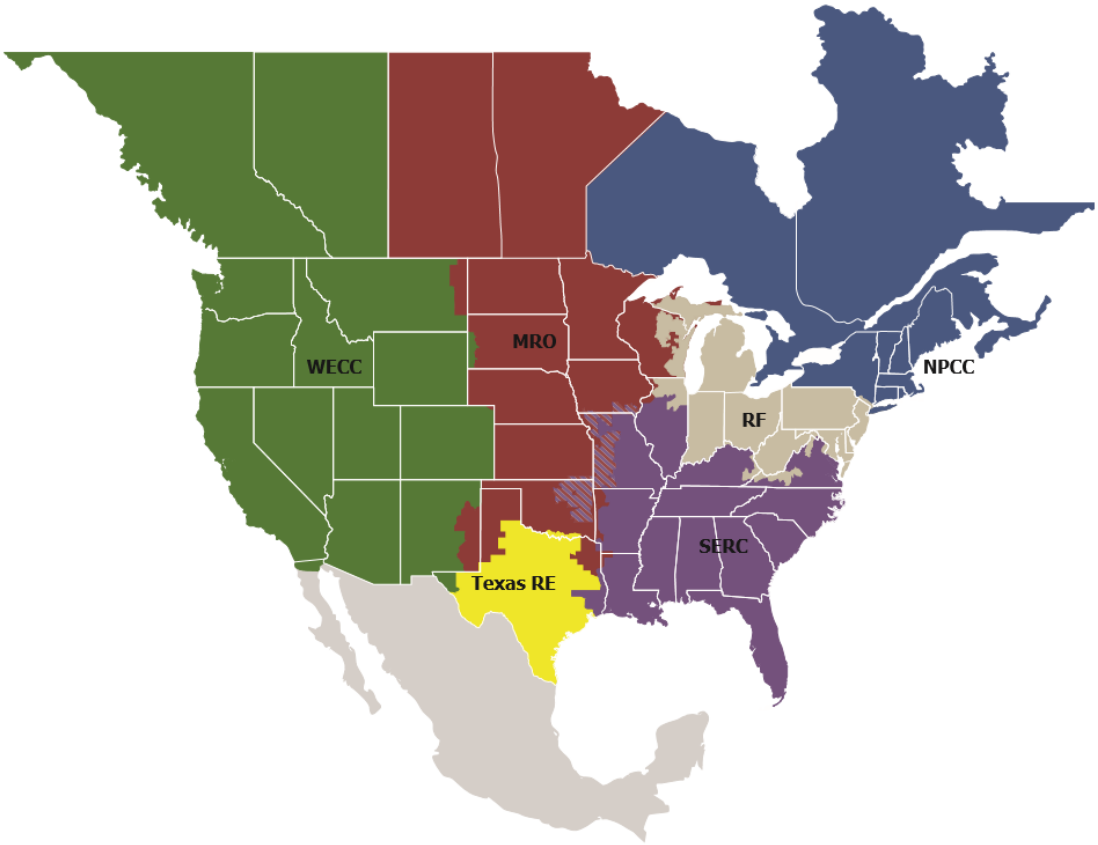
Preface

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

Acknowledgements

In addition to the efforts of NERC staff, the success of any report depends largely on the guidance and input of many others. NERC wishes to take this opportunity to express a special thanks to Carter Manucy at the Florida Municipal Power Agency for his exceptional contributions to the analysis of the data in this report. NERC also wishes to take this opportunity to express a special thanks to the Critical Infrastructure Protection Committee Supply Chain Working Group for their valuable contribution to developing the Supply Chain Risk Assessment Data Request authorized by the NERC Board of Trustees (Board). The authors also acknowledge and appreciate the significant contributions from individuals, working groups, subject matter experts, and organizations whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this assessment.

Executive Summary

Recognizing the complex and evolving nature of supply chain risks, NERC has undertaken various efforts to identify and mitigate potential risks. In particular, information and communications technology and industrial control systems may provide opportunities for adversaries to initiate cyberattacks, thereby presenting security risks to the Bulk Electric System (BES).[1] NERC is committed to using its many reliability tools to support industry's efforts to mitigate supply chain risks.

The risk to the BES from supply chain vulnerabilities lies in the increasing dependence of owners and operators on microelectronics, computer networks, and telecommunications. Complex control systems (such as those employed in the electric power industry) have become more sophisticated and complex, enabling better responsive control of the BES. The NERC critical infrastructure protection (CIP) Reliability Standards employ an asset-centric, risk-based approach to securing the BES. This approach requires systems or facilities that have the highest impact to the grid receive the highest level of protections while the lowest impact systems receive the fewest security requirements. This approach serves to mitigate the risk of threat actors targeting individual assets or electric power entities because of their potential impact to the grid. However, threats originating from supply chain vulnerabilities may challenge this asset-centric approach. The impact to the reliability of the BES could be significant if multiple owners and operators allow third-party access to their facilities and the associated BES Cyber Systems possess a common supply chain vulnerability. This type of compromise could result in aggregate misuse of numerous low impact BES Cyber Systems, which could potentially equal the impact of the compromise of any single high or medium impact BES Cyber System.

In 2017, NERC developed new and revised CIP Reliability Standards to help mitigate cyber security risks associated with the supply chain for high and medium impact 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 affect the BPS.

When adopting the Supply Chain Standards in August 2017, the NERC 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.

To better understand these risks, NERC collected data from registered entities pursuant to a request for data or information under Section 1600 of the NERC Rules of Procedure. This assessment documents the results of the analysis of the data to understand the implications of supply chain vulnerabilities not covered by the Supply Chain Standards and the extent of potential impacts (likelihood and risks to the BES). One observation was that most low impact assets reside in organizations with higher impact assets that are applicable to the approved Supply Chain Standards. This means that the low impact assets may be subject to the entity's supply chain risk management program and already have processes necessary to address supply chain vulnerabilities. However, many responders to the data request stated that their low impact BES Cyber Systems would be unaffected, especially for vendors that were not supplying high or medium impact BES Cyber Assets. The analysis is not aligned with the expectation in the NERC report that 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.

[1] Unless otherwise indicated, capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

The analysis also showed that the vast majority of transmission station and substation low impact BES Cyber Assets are at locations that have at most only one line greater than 300 kV or two lines greater than 200 kV (but less than 300 kV). Similarly, the vast majority of generation resource low impact BES Cyber Assets are at locations that have less than 500 MW. As such, an individual compromise to any one of these locations (transmission substations or generation resources) would generally be a localized event. However, a coordinated cyberattack with control of multiple locations could result in an event that has an interconnection wide BES reliability impact. One method to counter a coordinated cyberattack is to limit or eliminate third-party electronic access to these locations. Entities that have only low impact BES Cyber Systems allow third-party access to a significant number of their transmission stations and substations. While these locations represent a small percentage of all transmission stations and substation locations, the combined effect of a coordinated cyberattack on multiple locations could affect BES reliability beyond the local area. The analysis of third-party electronic access to generation resource locations is even more concerning. More than 50% of all low impact locations of generation resources allow third-party electronic access. As with transmission stations and substations, the combined effect of a coordinated cyberattack could greatly affect BES reliability beyond the local area.

Based on this information and analysis of NERC's data request, NERC staff recommends modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity.

Background

In recent years, the Federal Energy Regulatory Commission (FERC), NERC, and industry identified risks from the supply chain as a potential threat to BES reliability. Supply chains for information and communications technology and industrial control systems are long and multidimensional and involve numerous parties in a multitude of countries across the globe. In procuring products and services for their operations, BPS owners and operators typically rely on vendors and contractors that may use multiple third-party suppliers for components used in their products or technologies. Malicious actors may target one or more vendors in the supply chain to create or exploit vulnerabilities that could then be used to initiate cyberattacks on BES Cyber Systems and equipment.

On July 21, 2016, FERC issued Order No. 829,[2] directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations:

> "[FERC directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, discussed in detail [in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."[3]

Following the issuance of this order, NERC staff initiated Reliability Standards Project 2016-03 Cyber Security Supply Chain Risk Management to address supply chain risk management in the CIP Reliability Standards. The project resulted in the development of the Supply Chain Standards that consist of new Reliability Standard CIP-013-1 and modifications to Reliability Standards CIP-005-6 and CIP-010-3.

The Supply Chain Standards support reliability by requiring responsible entities to implement plans and processes to mitigate supply chain cyber security risks to high and medium impact BES Cyber Systems. Consistent with Order No. 829, the proposed Reliability Standards focus on the following four security objectives: software integrity and authenticity, vendor remote access protections, information system planning, and vendor risk management and procurement controls.

Reliability Standard CIP-013-1 requires responsible entities to develop and implement plans to address supply chain cyber security risks during the planning and procurement of high and medium impact BES Cyber Systems. Modifications in CIP-005-6 and CIP-010-3 bolster the protections in the currently-effective CIP Reliability Standards by addressing specific risks related to vendor remote access and software integrity and authenticity, respectively, in the operational phase of the system life cycle.

The Board adopted the Supply Chain Standards at its August 10, 2017, meeting. FERC approved the Supply Chain Standards with directives for additional modifications to address electronic access or control monitoring systems (EACMS) in Order No. 850, issued October 18, 2018.[4]

In its final report accepted by the NERC Board in May 2019,[5] 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

[2] Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards,* 156 FERC ¶ 61,050 (2016).
[3] *Id.* at P 2 (internal citation omitted); *see also id.* at PP 44–45.
[4] Order No. 850, *supra* note 1.
[5] NERC, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* (May 2019), available at https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NERC%20Supply%20Chain%20Final%20Report%20(20190517).pdf

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 connectivity[6] by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure. NERC staff worked with the CIPC Supply Chain Working Group to develop the questions in the data request.

NERC issued the request for data or information[7] in accordance with the expedited timing provisions of Section 1606 of the NERC Rules of Procedure, as the information was needed to evaluate a threat to the reliability or security of the BPS. On June 13, 2019, the Board authorized the use of shortened review and comment periods. NERC provided the data request to the FERC Office of Electric Reliability for information on June 24, 2019 and posted for public comment for a 20-day comment period from July 2–July 22, 2019. The Board approved the formal issuance of this data request on August 15, 2019. In accordance with Section 1600 of the NERC Rules of Procedure, the data request was mandatory for U.S. entities. Although not required, Canadian registered entities were encouraged to participate. NERC collected the data from August 19 through November 3. The results of this data request and analysis are provided in the following chapters.

[6] In this context, the phrase "external connectivity" refers to inbound or outbound electronic access, as defined in 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.
[7] NERC's Supply Chain Risk Assessment Data Request:
https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/Final%201600%20data%20request%20-%20clean.pdf

Chapter 1: Summary of Data Request Questions

Supply Chain Risk Assessment Data Request

In its May 17, 2019, report titled *Cyber Security Supply Chain Risks – Staff Report and Recommended Actions,* (Supply Chain Report), NERC staff 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."[8] The Supply Chain 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" (ERC).[9] NERC asked the following questions in the data request to achieve the objectives stated in the Supply Chain Report.

General Questions:

1. What are the NERC Compliance Registry numbers for which you are reporting under this Data Request?
2. Entity contact information
   a. Name:
   b. Title:
   c. Email address:
   d. Contact number:
3. CIP-002 Classifications.

CIP-002 Classifications	
Impact Rating	**Number of assets containing BES Cyber Systems**
High/Medium impact w/ ERC:	
Medium impact without ERC:	
Low impact:	
Low impact with external connectivity:[10]	

4. If you have medium or high impact BES Cyber Systems, please explain how your CIP-013-1 R1 plan will affect 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 do not 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:

[8] Supply Chain Report at 20.
[9] *Id.*
[10] In this context, the phrase "external connectivity" refers to inbound or outbound electronic access, as defined in 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.

The following information was provided to assist in answering Questions 3–5:

> NERC needed to understand the basis for each entity's answer in order to understand the data received from the data request. How each entity categorized its BES Cyber Systems could have a large impact on survey results. To have useable and comparable results, the common basis was the six locations highlighted in CIP-002. The data request focused on those locations and not how entities designed their BES Cyber Systems.
>
> In the Supply Chain Report, NERC staff stated that they expected the following: 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 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"[11] referred to physical space associated with an asset. 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. For example, if a substation contains both medium and low impact BES Cyber Systems, the entity 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. For each location in the response to Question 6, entities were to provide an estimate of the low impact assets identified pursuant to CIP-002 R 1.3.

6. For each location identified, answer the following questions. You may group assets with the same answers into a single line item. Note "inbound or outbound 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.

Low Impact Risk Assessment by Locations												
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[12]	**2**	**3**	**4**	**2**	**3**	**4**	**2**	**3**	**4**	**2**	**2**	**1**
a. Number of locations with low impact BES Cyber Systems												
b. Number of locations with inbound or outbound connectivity to a BES Cyber System												
c. Number of locations with dial up												

[11] 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.

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

Low Impact Risk Assessment by Locations												
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[12]	**2**	**3**	**4**	**2**	**3**	**4**	**2**	**3**	**4**	**2**	**2**	**1**
connectivity to a BES Cyber System												
d. Number of locations allowing third-party remote access[13] to a BES Cyber System												
e. Number of locations with third-party monitoring of a BES Cyber System[14]												
f. Number of locations with constant monitoring[15] of remote connectivity to a BES Cyber System												
g. Number of locations participating in government/industry programs[16]												
h. Number of locations with NO external routable connectivity and NO dial up connectivity to a BES Cyber System												

The following information was provided to assist in answering Question 6.

> 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 was developed. 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

[13] 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).

[14] 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.

[15] 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.

[16] 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).

to low impact BES Cyber Assets, an entity needed to 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 containing different or multiple assets, they were instructed to use the first criterion that applies (i.e., count each location once) in the below table to determine its associated risk score.

Location Risk Score Table			
Criterion (See CIP-002 Attachment 1)	**Description**	**Risk Criterion**	**Location Risk Score**
3.1	Control Centers / backup Control Centers[17]	MW of load and/or generation controlled	0–500 MW = 2 501–1,000 MW = 3 1,001-1,500 MW = 4
3.2	Transmission stations and substations	MVA/Criterion 2.5 Score	0–1400 = 2 1,401–2,000 = 3 2,001–3,000 = 4
3.3	Generation resources[18]	MW per location	0–500 MW = 2 501–1,000 MW = 3 1,001–1,500 MW = 4
3.4	Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements[19] 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

CIP-013 Cost of Implementation:
The following information was provided to assist entities in 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.

[17] These are low impact Control Centers per CIP-002-5.1a that only apply to some BAs and GOPs.
[18] If your entity has performed generation segmentation and created multiple low impact BES Cyber Systems, account for them as individual low impact BESCS locations (four units would count as four locations) as per your CIP-002. Do not double-count under medium impact under Question 3 and again as low impact under Question 5.
[19] If this includes generation counted under 3.3, do not count again under 3.4

- 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.

7. Do you agree with the above SME assessment—Yes or No?

Provide CIP-013 cost or benefit amounts should you answer "no" to the above question:

Overview of Responses

This section provides an overview of the responses received from the data request.

Questions 1–3: NERC received responses from 1,040 entities.[20] 654 of these (63%) had only locations with low impact BES Cyber Assets with the remainder (386 or 37%) having a combination of locations that contained high, medium, and low impact BES Cyber Assets. The analysis of responses for question 3 is provided in Chapter 2.

Question 4: When those entities that had a combination of high, medium, and low impact BES Cyber Assets were asked about how their CIP-013-1 R1 plan will affect their low impact BES Cyber Systems, responses were mixed. Some stated that they plan to use a documented enterprise-wide supply chain cyber security risk management plan, which would include all Cyber Assets regardless of impact rating criteria. Others stated that their low impact BES Cyber Systems would be unaffected, especially for vendors that were not supplying high or medium impact BES Cyber Assets. This is contrary to the expectation in the Supply Chain Study that 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.

Question 5: When those entities that had only low impact BES Cyber Assets were asked how they currently plan on mitigating Supply Chain Management risks, many stated that they would use only trusted vendors and/or develop a supply chain risk list. Many entities stated that the list would be developed by using a common risk assessment across those vendors. Others planned to rely on information from NERC's Electricity Information Sharing and Analysis Center to identify known vulnerabilities and potential supply chain issues. Many planned to control risk through processes developed for compliance with CIP-003. Some have taken the position that since no requirements exist mandating the mitigation of Supply Chain Management risks for low impact BES Cyber Systems, they do not intend to implement any plan to mitigate the risks. This lack of consistency on this risk assessment means that there is no certainty across industry that there are consistent supply chain protections. Therefore, a coordinated cyberattack with control of multiple locations could result in an event that has an interconnection wide BES reliability impact.

Question 6: The analysis of responses for question 6 is provided in Chapter 2.

Question 7: The Supply Chain Working Group developed a draft response to the cost to implement the Supply Chain Standards, which was provided in the data request and entities were asked if they agreed with the statement. More than 99% of the responders agreed with the draft response that it was premature for CIP-013 registered entities to

[20] While there are over 1,400 registered entities, many are not subject to the CIP standards and thus are not required to respond to the survey. The respondents represented those that were subject to the CIP standards.

determine or estimate costs or benefits associated with the implementation of the standard based on the list of factors provided.

Chapter 2: Analysis of Data

Comparison of BES Cyber Asset locations

NERC needed to understand the basis for each entity's answer in order to understand the data received from the data request. How each entity categorized its BES Cyber Systems could have a large impact on these survey results. For comparison and to have a common basis, NERC used the asset locations referenced in CIP-002-5.1.a:

i. Control Centers and backup Control Centers

ii. Transmission stations and substations

iii. Generation resources

iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements

v. Special Protection Systems that support the reliable operation of the BES;

vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1.

The data request focused on asset locations and not how entities designed their BES Cyber Systems.

Figure 2.1 provides a summary of the responses to question 3. Approximately 87% of all locations have low impact BES Cyber Systems, and many of those locations have external connectivity (defined as inbound or outbound electronic access) as defined in CIP-003-7, Attachment 1, Section 3. The BES Cyber Systems located at these locations would not be subject to the current Supply Chain Standards.

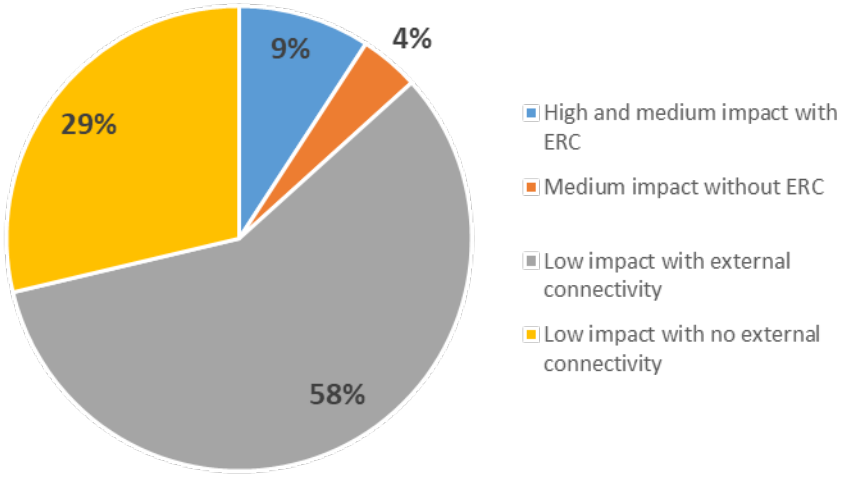


Figure 2.1: All Locations Containing BES Cyber Systems

NERC differentiated the responses based on entities that had a combination of locations of high, medium, and low impact BES Cyber Systems compared to entities that had only locations of low impact BES Cyber Systems. **Figure 2.2** shows the data for entities with a combination of locations. Note that the percentages are relatively close to those in **Figure 2.1**. In other words, most of the locations are at entities that have a combination of locations of high, medium, and low impact BES Cyber Systems. NERC then contrasted with responses from entities that had only locations of low impact BES Cyber Systems, which **Figure 2.3** shows. Note that two-thirds of these low impact BES Cyber Systems locations had external connectivity. In addition, when comparing connectivity across impact categories, the ratio of external connectivity to no external connectivity remained consistent at two-to-one.

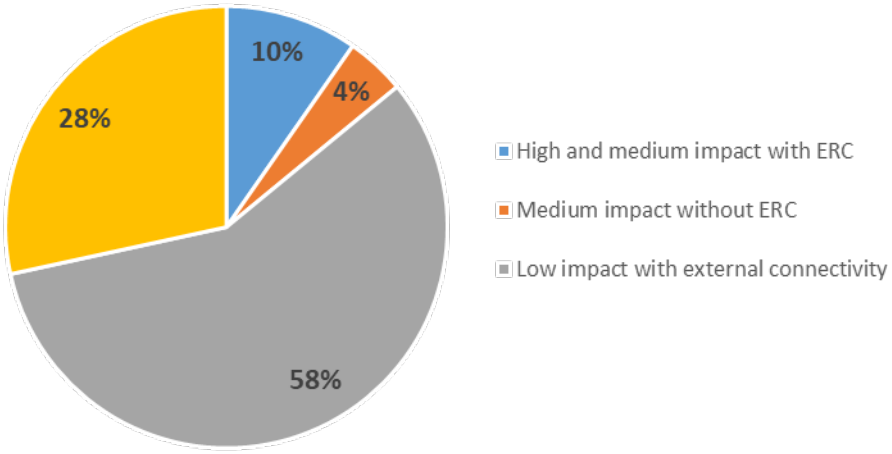


Figure 2.2: Locations for Entities with High, Medium, and Low Impact BES Cyber Systems

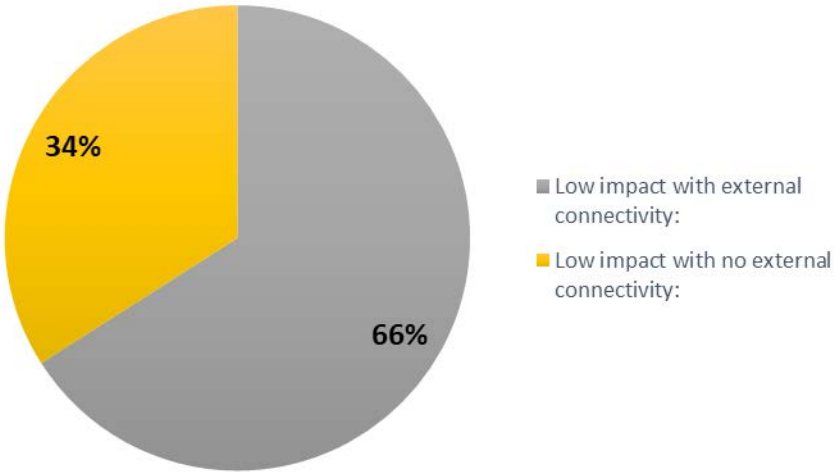


Figure 2.3: Locations for Entities with only Low Impact BES Cyber Systems

NERC then examined the data to determine whether entities allowed inbound or outbound connectivity at locations with low impact BES Cyber Systems. **Figure 2.4** shows the data for entities that have a combination of low, medium, and high impact BES Cyber Systems. The predominance of locations are transmission stations and substations as well as generation resources. In addition, a significant percentage of those entities allow inbound or outbound connectivity. **Figure 2.5** shows the data for entities that have only low impact BES Cyber Systems. Again, the predominance of locations are transmission stations and substations as well as generation resources, with a significant percentage of those locations allowing inbound or outbound connectivity. Further generation resources that allow inbound or outbound connectivity outnumber the transmission stations and substations in this dataset.

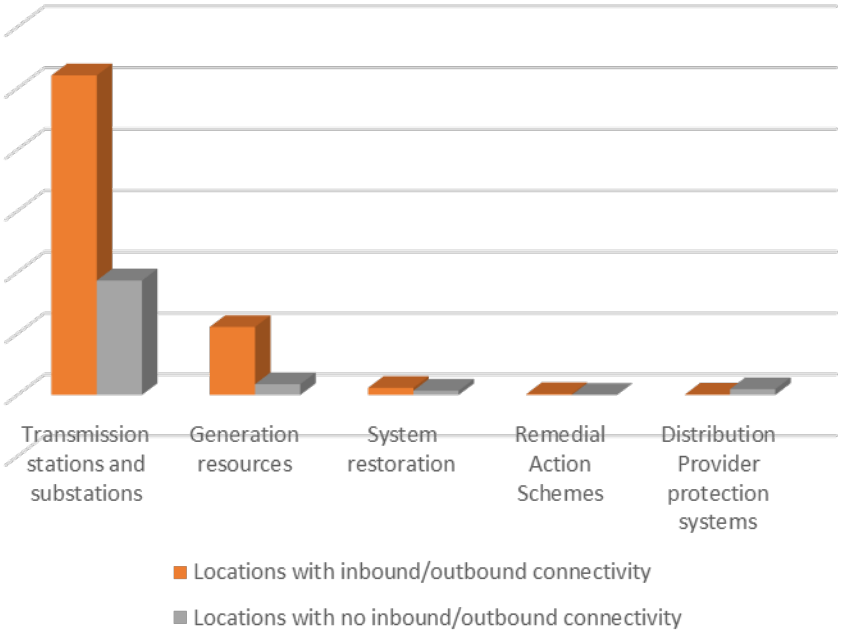


Figure 2.4: Locations for Entities with High, Medium, and Low Impact BES Cyber Systems

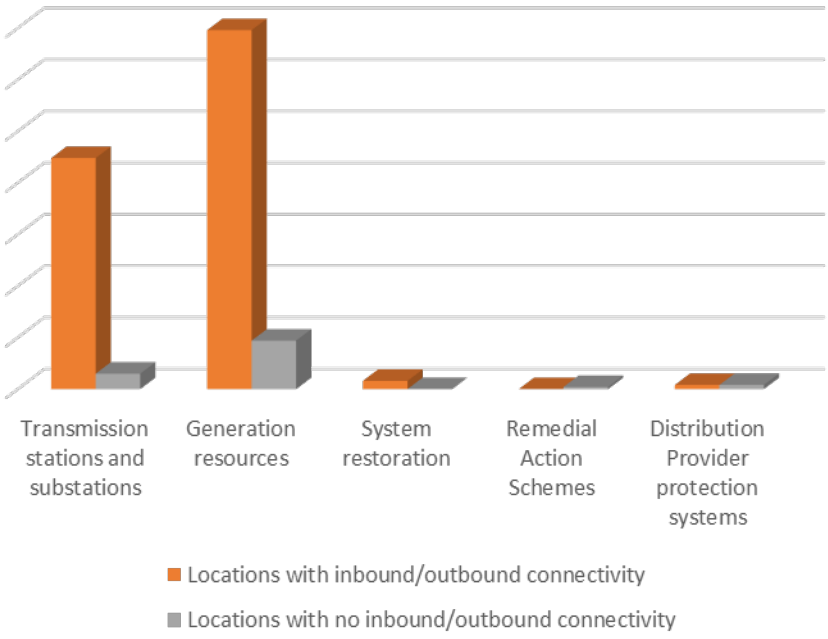


Figure 2.5: Locations for Entities with only Low Impact BES Cyber Systems

Since third-party access is a security risk, especially when it comes to supply chain vulnerabilities, NERC examined the data to determine whether an entity allowed third-party access at locations with low impact BES Cyber Systems. **Figure 2.6** shows the data for transmission stations and substations for entities that have a combination of low, medium, and high impact BES Cyber Systems. The vast majority of these locations do not allow third-party access, no matter the MVA criteria as established in criterion 3.2 in the data survey. **Figure 2.7** shows the data for transmission stations and substations for entities that have only low impact BES Cyber Systems. A significant percentage of these locations **do** allow third-party access, but only for the lowest location risk score as established in criterion 3.2 in the

data survey. In addition, while no values are presented in this report, the total number of locations represented in **Figure 2.7** represents only 3% of all transmission stations and substations locations reported low impact BES Cyber Systems. While these locations represent a small percentage of all transmission stations and substation locations, the combined effect of a coordinated cyberattack on multiple locations could impact BES reliability beyond the local area.

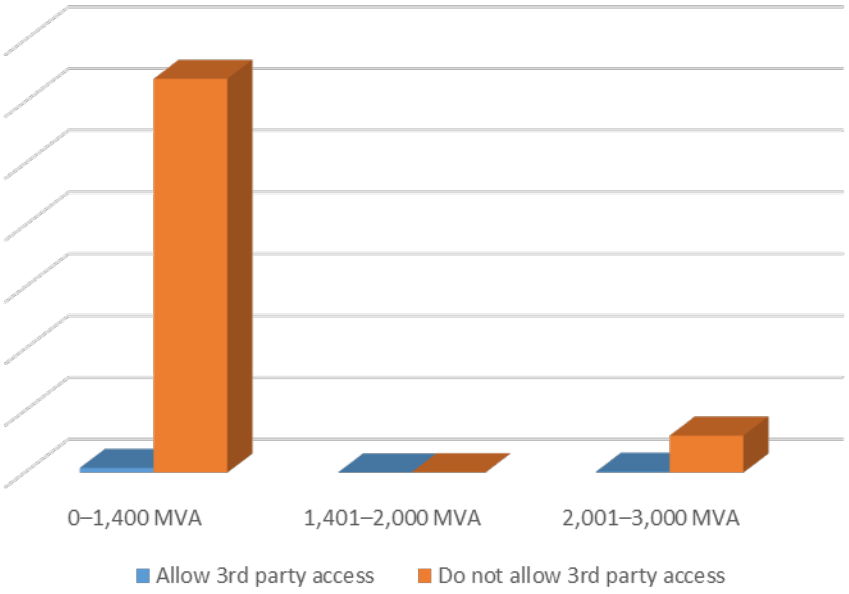


Figure 2.6: Transmission Stations and Substations for Entities with High, Medium, and Low Impact BES Cyber Systems

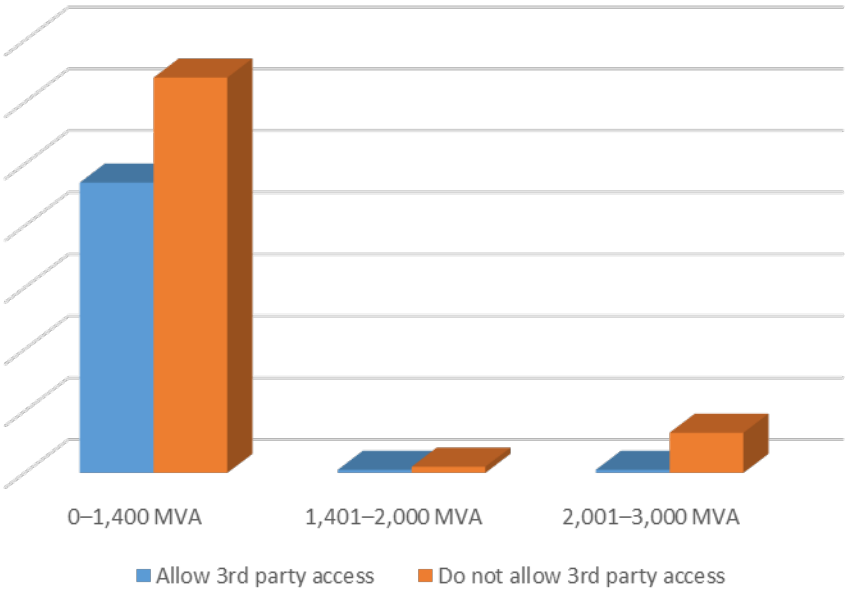


Figure 2.7: Transmission Stations and Substations for Entities with only Low Impact BES Cyber Systems

Likewise, NERC examined the data to determine whether third-party access was allowed at generation resource locations with low impact BES Cyber Systems. **Figure 2.8** shows the data for generation resources for entities that have a combination of low, medium, and high impact BES Cyber Systems. More of these generation locations, with less than 500 MW, allow third-party access than do not. **Figure 2.9** shows the data for generation resources for entities that have only low impact BES Cyber Systems. A significant percentage of these locations allow third-party access. In addition, while no values are presented in this report, the total number of locations represented in **Figure 2.9** represents 23% of all generation resource locations reported with low impact BES Cyber Systems. This is a significantly higher percentage than that represented by transmission stations and substations. As with transmission stations and substations, the combined effect of a coordinated cyberattack could greatly affect BES reliability beyond the local area.

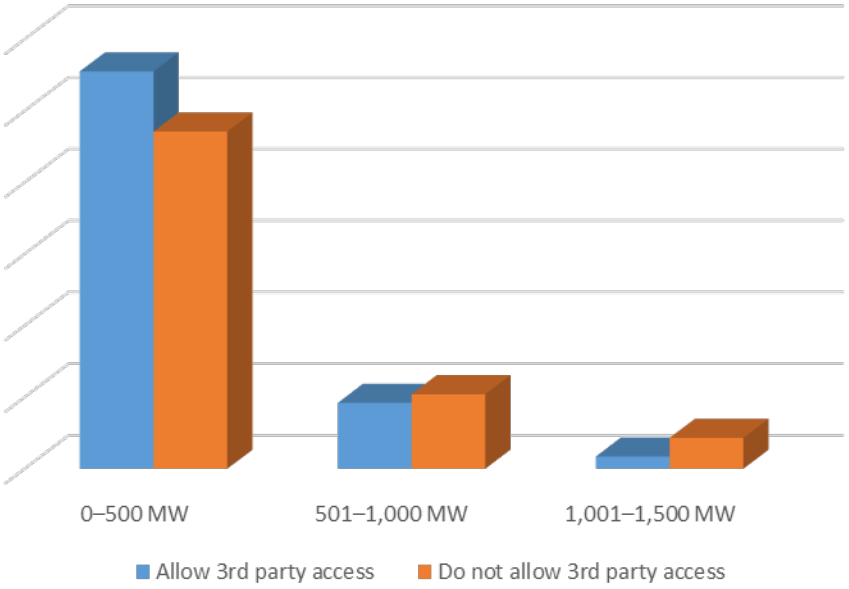


Figure 2.8: Generation Resources for Entities with High, Medium, and Low Impact BES Cyber Systems

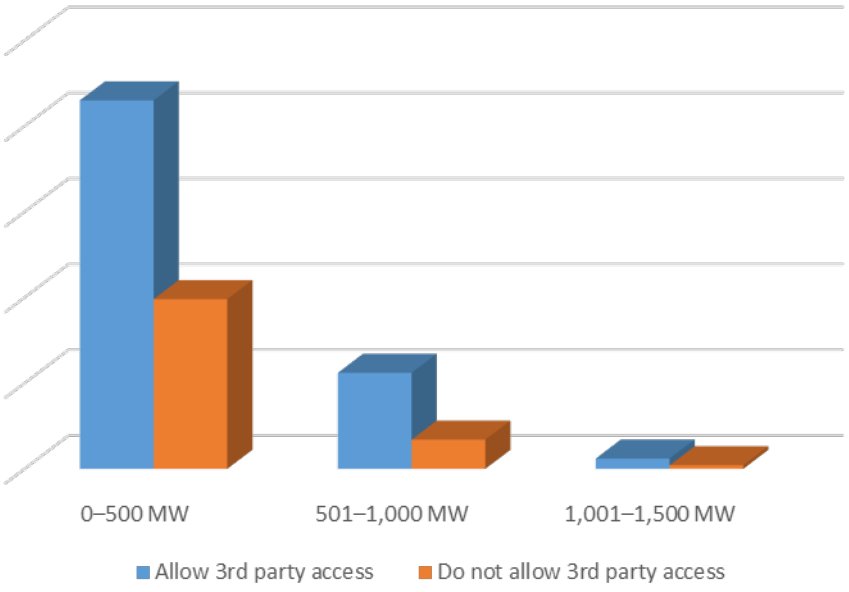


Figure 2.9: Generation Resources for Entities with only Low Impact BES Cyber Systems

Chapter 3: Conclusion

Supply chain compromise of industrial control system hardware, software, and computing and networking services associated with BES operations could pose a threat to BES reliability. The Supply Chain Standards require responsible entities that possess high and medium impact BES Cyber Systems to develop processes to manage supply chain risks through the procurement process. The Supply Chain Standards as currently approved apply to the higher-risk systems that have the greatest impact to the grid.

Based on the analysis of the data and in consideration of the common device supply chain risk, NERC staff recommends the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity.

When assessing the data, NERC staff made a few observations. First, most low impact assets reside in organizations with higher impact assets that are applicable to the approved Supply Chain Standards. The analysis of the data is contrary to the expectation in the Supply Chain Study that entities possessing 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. Namely, when asked in the survey how their CIP-013-1 R1 plan will affect their low impact BES Cyber Systems (Question 4 of the data request), entities provided inconsistent responses. Some stated that they plan to use a documented enterprise-wide Supply Chain Cyber Security Risk Management plan that includes all BES Cyber Systems (high/medium/low). Others stated that they do not intend to apply their supply chain risk management plans to their low impact BES Cyber Systems, especially involving vendors that were not supplying high or medium impact BES Cyber Assets.

Another observation was that most low impact BES Cyber Asset locations are individually lower risk based on the location risk score table in the survey. The vast majority of transmission station and substation low impact BES Cyber Assets are at locations that have only one line greater than 300 kV at most or two lines greater than 200 kV but less than 300 kV. Similarly, the vast majority of generation resource low impact BES Cyber Assets are at locations that have less than 500 MW. An individual compromise to any one of these locations (transmission station and substation or generation resource) would generally be a localized event. However, a coordinated cyberattack with control of multiple locations could result in an event that has an interconnection-wide BES reliability impact.

One method to counter a coordinated cyberattack is to limit or eliminate third-party electronic access to locations. NERC observed entities that have a combination of low, medium, and high impact BES Cyber Systems in transmission stations and substations generally do not allow third-party access. However, entities that have only low impact BES Cyber Systems mostly allow third-party access to a significant number of their transmission stations and substations. As noted in **Chapter 2**, these locations represent only 3% of all transmission stations and substation locations reported with low impact BES Cyber Systems. That said, the combined effect of a coordinated cyberattack at multiple locations could impact BES reliability beyond their local area; this is an area of concern.

The analysis of third-party electronic access to generation resource locations is even more concerning. More than 50% of all generation resource locations allow third-party electronic access, whether entities have only low impact BES Cyber Systems or a combination of low, medium, and high impact BES Cyber Systems. As with transmission stations and substations, the combined effect of a coordinated cyberattack could greatly impact BES reliability beyond the local area.