NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 2, 2020

Mr. Greg Ford, Chair
NERC Member Representatives Committee

Dear Greg:

I invite the Member Representatives Committee (MRC) to provide policy input on two matters of particular interest to the NERC Board of Trustees (Board) as it prepares for its February 5-6, 2020, meetings in Manhattan Beach, California. In addition, policy input is requested on any items on the preliminary agendas for the quarterly Board, Board Committees, and MRC meetings. The preliminary agendas are included in the MRC Informational Session agenda package (see Item 1) and are attached hereto (**Attachment A**). Because final agenda packages with background materials are posted after policy input is due, the MRC's agenda includes an opportunity for MRC members to provide additional input to the Board on the final agenda and materials. **As a reminder, please include a summary of your comments in your response (i.e., a bulleted list of key points) for NERC to compile into a single summary document to be provided to the Board for reference, together with the full set of comments.**

Electromagnetic Pulse Strategic Recommendations

Protecting the bulk power system (BPS) and achieving effective reduction of reliability risk is integral to the Electric Reliability Organization mission. Recognizing the risk potential from electromagnetic pulses (EMPs), NERC launched an effort to better understand reliability concerns associated with EMPs and to identify ways to enhance resilience in the face of these concerns. NERC created the EMP task force in April 2019 to identify key issues and scope opportunities for action. At its November 2019 meeting, the Board accepted the EMP task force's report that included a series of strategic recommendations. Recognizing the broad expanse of the recommendations in the report and NERC's focus on effectiveness and efficiency, the Board asked NERC staff to propose which recommendations should be pursued first and EMP priorities for the ERO Enterprise for the long term. In response, NERC staff is recommending that the EMP Task Force should be maintained and serve under the new Reliability and Security Technical Committee (RSTC) with a specific workplan. NERC staff also proposes the following priorities for addressing the other recommendations in the report. Each section is provided in prioritized order. Items that NERC staff has identified as the highest overall priority, and thus should be addressed in the near term, are provided in **bold**.

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

Policy priorities:

1. **The EMP Task Force should establish performance expectations for the BPS regarding a predefined EMP event. NERC staff will work with other agencies on areas that require coordination.**
2. The EMP Task Force should develop guidance for the electric industry on interdependent utility sector coordination related to an EMP event.
3. The ERO Enterprise should develop educational materials about EMPs and their impact to electronic devices and BPS stability to inform industry and other interested parties.

Research and Development priorities:

1. **The ERO Enterprise should support additional research to close existing knowledge gaps into the complete impact of an EMP event to understand vulnerabilities, develop mitigation strategies, and plan response and recovery efforts.**
2. The EMP Task Force should work with other standards setting organizations (e.g. IEEE, Underwriters Laboratories) to designate equipment specifications for the electric sector utility industry around EMP hardening and mitigation strategies.
3. The ERO Enterprise should monitor and communicate to the industry research pertaining to EMP and EMP-related national security initiatives that impact the BPS.

Vulnerability Assessments priorities:

1. **The ERO Enterprise should develop tools and methods for system planners and equipment owners to use in assessing EMP impacts on the BPS.**
2. **The EMP Task Force should provide guidance to industry on how to identify and prioritize hardening of assets that are needed to maintain and restore critical BPS operations.**

Mitigation Guideline priorities:

1. The EMP Task Force should develop guidelines for industry to use in developing strategies for mitigating the effects of an EMP on the BPS (control centers/plant controls, substations, and power plants).

Response and Recovery priorities:

1. **The EMP Task Force should develop guidance for supporting systems and equipment (including spare equipment strategy) needed for BPS recovery in a post-EMP event.**
2. The EMP Task Force should develop response planning guidelines for EMP event pre and post-contingency actions that aligns with plans of applicable regulatory authorities.
3. The EMP Task Force should develop criteria to incorporate into operating plans and procedures and system restoration plans actions pertaining to EMP event.

4. The RSTC should develop training for system and plant operators about EMP events and consider incorporating EMP events in coordinated industry exercises to test response planning and system restoration recovery efforts.
5. The ERO Enterprise should work with the appropriate agencies to develop a real-time national notification system for the electric sector to System Operators and Plant Operators pertaining to an EMP event and its parameters.

The ERO Enterprise will facilitate conversations with appropriate agencies to encourage the development of solutions to the following policy matters outside of its scope:

- Cost recovery mechanisms for planning, mitigation, and recovery plans required to be developed.
- Access to necessary research by key industry personnel with security clearances (at the appropriate levels) conducted by the National Labs, Defense Threat Reduction Agency, and any additional third-party research on electric utility equipment by the Department of Energy.
- Access to industry-relevant information on E1, E2, and E3 EMP environments and other necessary related research.

The Board requests MRC policy input on the following:

1. **Do you agree with the recommendations above?**
2. **Do you agree with the priority levels proposed by NERC staff to address the recommendations?**
3. **Are there any additional recommendations related to EMP that the Board should consider?**

Supply Chain Risk Assessment

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.

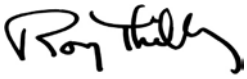
Based on the analysis of the data request outlined in the *Supply Chain Risk Assessment* (**Attachment B**), NERC staff is recommending modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity.

The Board requests MRC policy input on the following:

1. **Do you agree with the recommendation?**
2. **Is there an alternate way to address the identified risk in a more cost effective manner?**

Written comments in response to the input requested above, the preliminary agenda topics, and on other matters that you wish to bring to the Board's attention are due by **January 22, 2020,** to Kristin Iwanechko, MRC Secretary (Kristin.Iwanechko@nerc.net). The formal agenda packages for the Board, Board Committees, and MRC meetings will be available on January 23, 2020, and the presentations will be available on January 30, 2020. The Board looks forward to your input and discussion of these matters during the February 2020 meetings.

Thank You,



Roy Thilly, Chair
NERC Board of Trustees

cc: NERC Board of Trustees
Member Representatives Committee

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Member Representatives Committee (MRC)

Pre-Meeting and Informational Webinar

January 9, 2020

RELIABILITY | RESILIENCE | SECURITY




Objectives – Pre-Meeting and Informational Session

- Review preliminary agenda topics for:
  - February 5 MRC meeting
  - February 5-6 Board of Trustees and Board Committee (open) meetings
- Review policy input letter topics
- Receive updates on emerging and informational issues

Schedule of Quarterly NERC Meetings and Conference Calls

Wednesday, February 5, 2020	
7:00-8:00 a.m. **Room name:**	Public Breakfast
8:00-9:00 a.m. **Room name:**	Corporate Governance and Human Resources Committee Meeting —**Open**
9:15-10:15 a.m. **Room name:**	Compliance Committee Meeting —**Open**
10:30-11:00 a.m. **Room name:**	Finance and Audit Committee—**Open**
11:00 a.m.-12:00 p.m. **Room name:**	Technology and Security Committee—**Open**
12:00-1:00 p.m. **Room name:**	Lunch
1:00-5:00 p.m. **Room name:**	Member Representatives Committee Meeting—**Open**
5:30-7:00 p.m. **Room name:**	Reception
Thursday, February 6, 2020	
7:30-8:30 a.m. **Room name:**	Public Breakfast
8:30 a.m.-12:00 p.m. **Room name:**	Board of Trustees Meeting—**Open**

**Times are tentative and subject to change*

Corporate Governance and Human Resources Committee
8:00 a.m. – 9:00 a.m., February 5

- Approve Board Committees' Self-Assessment Surveys
- 2020 Board of Trustees Committee, Chair and Chair-Elect/Vice Chair Appointments
- Review 2020 Work Plan Priorities for Board of Trustees Approval
- Review 2019 Work Plan Priorities Year-End Report
- Review Board Self-Assessment and MRC Assessment of Board of Trustees Effectiveness Results and Work Plan
- Annual Review of NERC Governance Guidelines
- Review Annual Conflict of Interest and Independence Report
- Annual Review of Committee Mandate
- Human Resources and Staffing Update

Compliance Committee
9:15 a.m. – 10:15 a.m., February 5

- Compliance Monitoring and Enforcement Program Annual Report
- Annual Review of Committee Mandate
- Critical Infrastructure Protection Discussion

Finance and Audit Committee
10:30 a.m. - 11:00 a.m., February 5

- 2019 Year-End Unaudited Results of Operations
- Annual Review of Investment Performance
- Annual Review of Executive Management Expenses Policy
- Annual Review of Committee Mandate

Technology and Security Committee
11:00 a.m. – 12:00 p.m., February 5

- ERO Enterprise Information Technology Strategy and IT Projects Update
- E-ISAC Update
- Annual Review of Committee Mandate

Member Representatives Committee
1:00 p.m. - 5:00 p.m., February 5

- Election of NERC Trustees
- General Updates and Reports
  - Business Plan and Budget Input Group Update
  - Regulatory Update
  - Reliability and Security Technical Committee Update
  - ERO Enterprise Effectiveness Survey Next Steps
- Policy and Discussion Items
  - Responses to the Board's Request for Policy Input
    - EMP Strategic Recommendations
    - Supply Chain Risk Assessment
  - Additional Policy Discussion of Key Items from Board Committee Meetings
  - MRC Input and Advice on Board Agenda Items and Accompanying Materials

Member Representatives Committee
1:00 p.m. - 5:00 p.m., February 5

- Technical Updates
  - Update on FERC Reliability Matters
  - Grid Transformation
    - Framework to Address Known and Emerging Reliability and Security Risks
    - Panel on Reliability Impacts of Grid Transformation

Board of Trustees
8:30 a.m. - 12:00 p.m., February 6

- Committee Membership and Charter Amendments
  - Reliability and Security Technical Committee Membership
  - Reliability Issues Steering Committee Membership
  - Critical Infrastructure Protection Committee Membership
  - Personnel Certification Governance Committee Membership and Charter Amendments
- NIAC Update and Recommendations to the President, William Fehrman, Vice Chair, MEC
- Report on Board of Trustees February 4, 2020 Closed Session and ISO NE Joint Board Meeting
- Board of Trustees Self-Assessment Results

Board of Trustees
8:30 a.m. - 12:00 p.m., February 6

- Election and Appointment of Board Chair and Chair-Elect/Vice Chair, Board Committee Assignments and NERC Officers
- Board Self-Assessment and MRC Assessment of Board Effectiveness Survey and Board Committee Self-Assessments
- Board Committee Reports
  - Approve 2020 Work Plan Priorities
  - Accept 2019 Year-End Unaudited Results of Operations
- Standards Quarterly Report and Actions
  - Adopt Project 2017-07 Standards Alignment with Registration
  - Adopt Modifications to PRC-024-2, TPL-007-3, and CIP-002-6
  - Adopt BAL-001-TRE-2

Board of Trustees
8:30 a.m. - 12:00 p.m., February 6

- Other Matters and Reports
  - Discuss Policy Input and Member Representatives Committee Meeting
  - Approve EMP Report Recommendations
  - Approve Supply Chain Recommendations
  - Approve Retirement of CCCPP-002 Compliance Monitoring Program for Reliability Standards Applicable to NERC
  - Approve CCCPP-010 Criteria for Annual Regional Entity Program Evaluation Revisions
  - Update on 2019 and 2020 ERO Enterprise Dashboards
  - Update on Reliability Coordinator Function in the Western Interconnection
- Committee, Forum, and Group Reports
  - Approve Standards Committee 2020 Work Plan
  - Approve Compliance and Certification Committee 2020 Work Plan

January 9 – MRC Informational Session

- Overview of Policy Input Letter
  - EMP Strategic Recommendations
  - Supply Chain Risk Assessment
- Reliability and Security Technical Committee Update

Upcoming Dates

- **January 2:** Policy input letter issued
- **January 22:** Written comments due on policy input topics and preliminary agenda topics
- **January 23:** Board and MRC agenda packages and policy input letter comments posted
- **January 30:** Board and MRC presentations posted

Questions and Answers

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

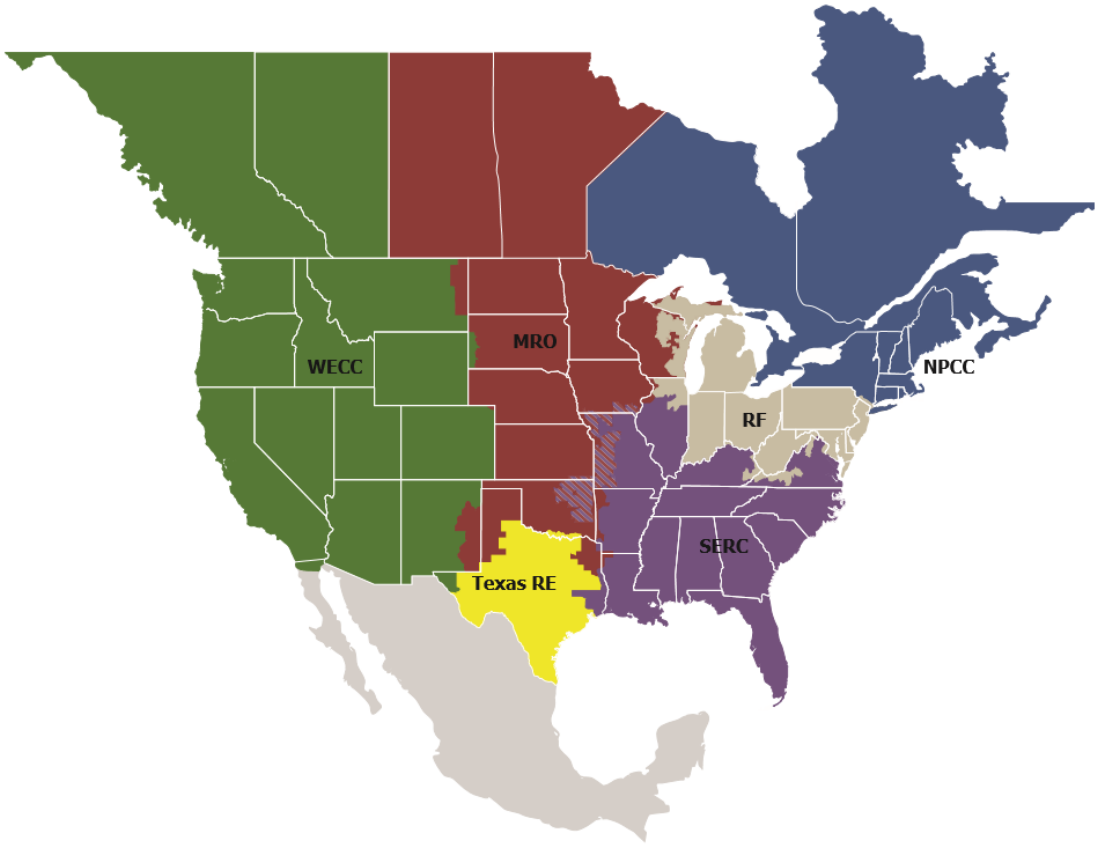
Preface

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.

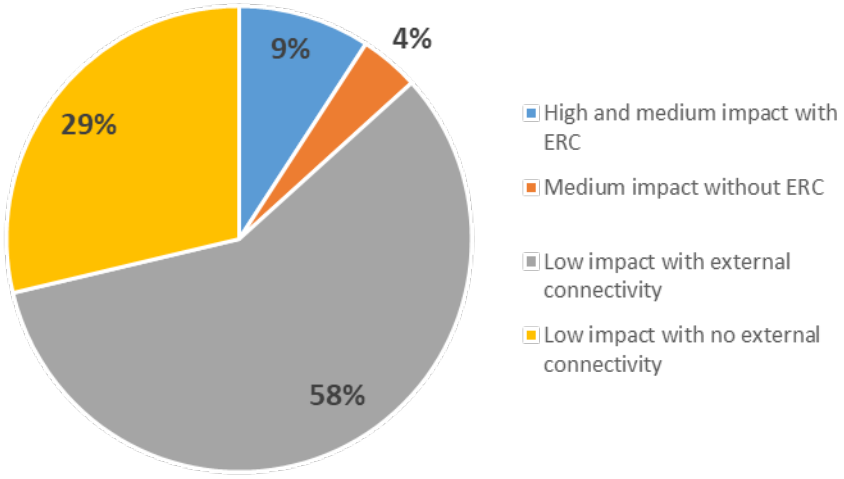


Figure 2.1: All Locations Containing BES Cyber Systems

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.

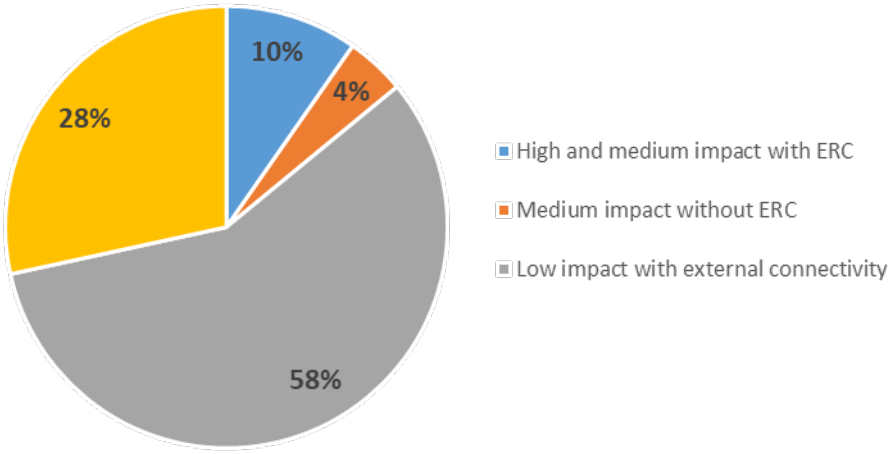


Figure 2.2: Locations for Entities with High, Medium, and Low Impact BES Cyber Systems

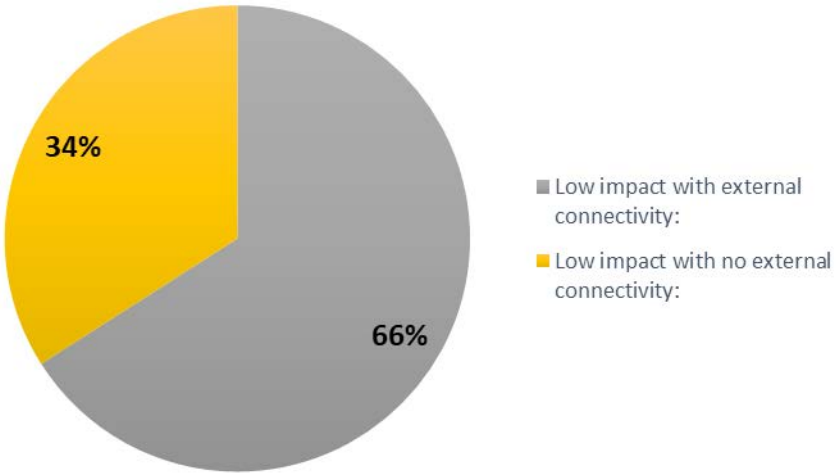


Figure 2.3: Locations for Entities with only Low Impact BES Cyber Systems

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.

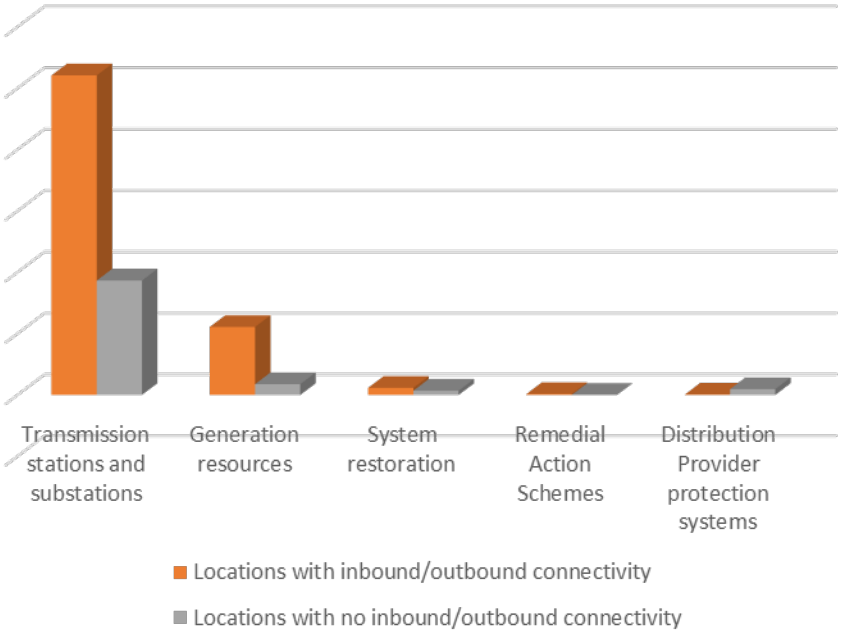


Figure 2.4: Locations for Entities with High, Medium, and Low Impact BES Cyber Systems

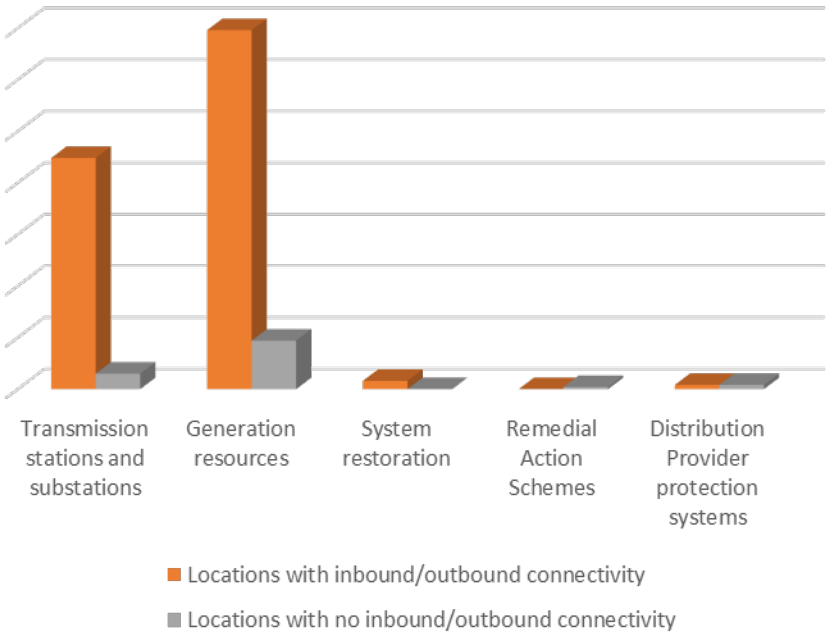


Figure 2.5: Locations for Entities with only Low Impact BES Cyber Systems

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.

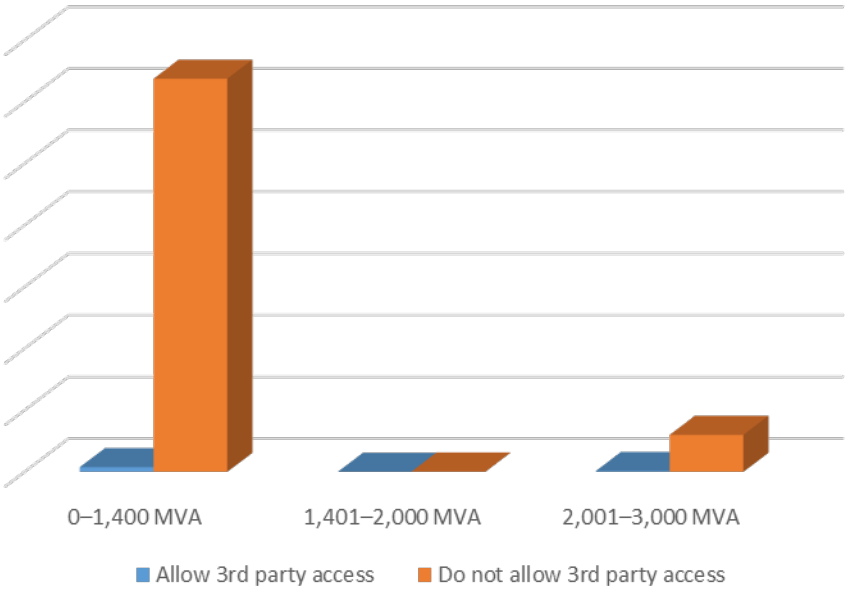


Figure 2.6: Transmission Stations and Substations for Entities with High, Medium, and Low Impact BES Cyber Systems

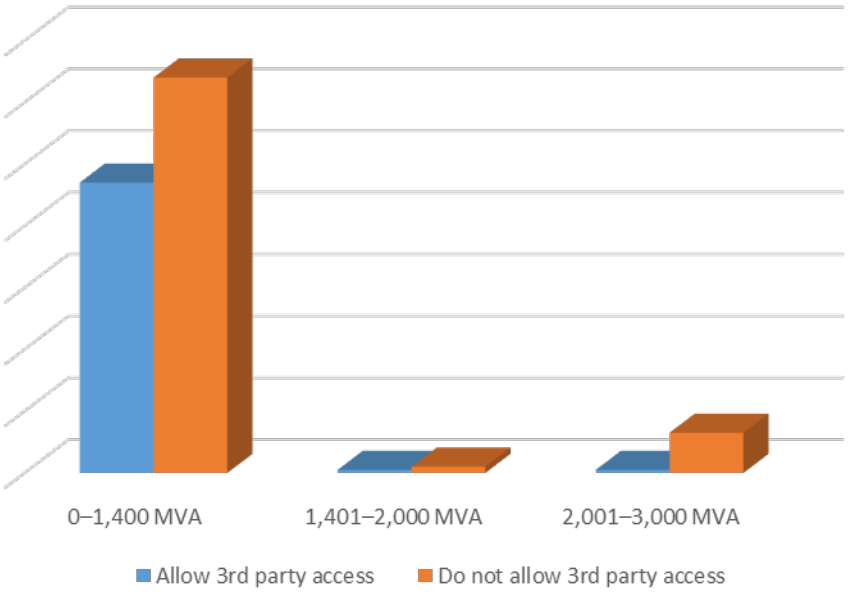


Figure 2.7: Transmission Stations and Substations for Entities with only Low Impact BES Cyber Systems

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.

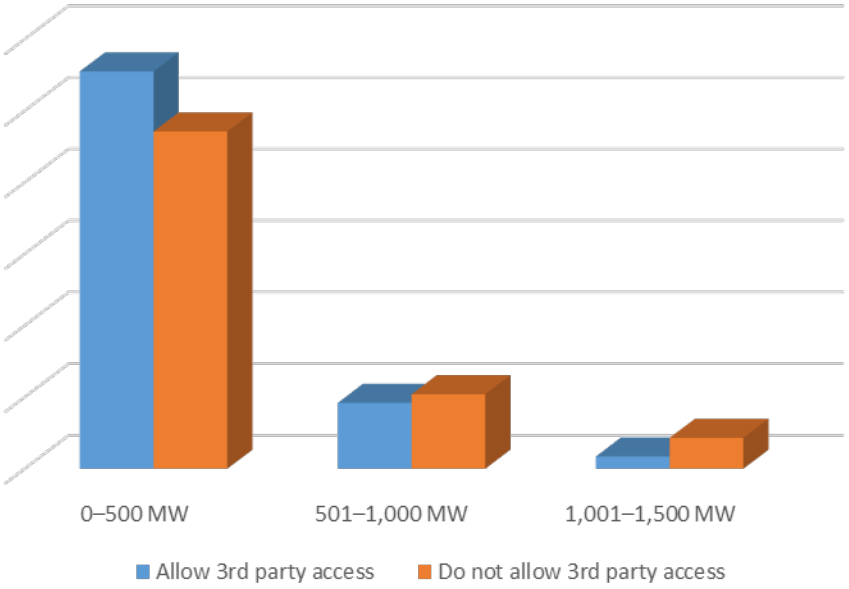


Figure 2.8: Generation Resources for Entities with High, Medium, and Low Impact BES Cyber Systems

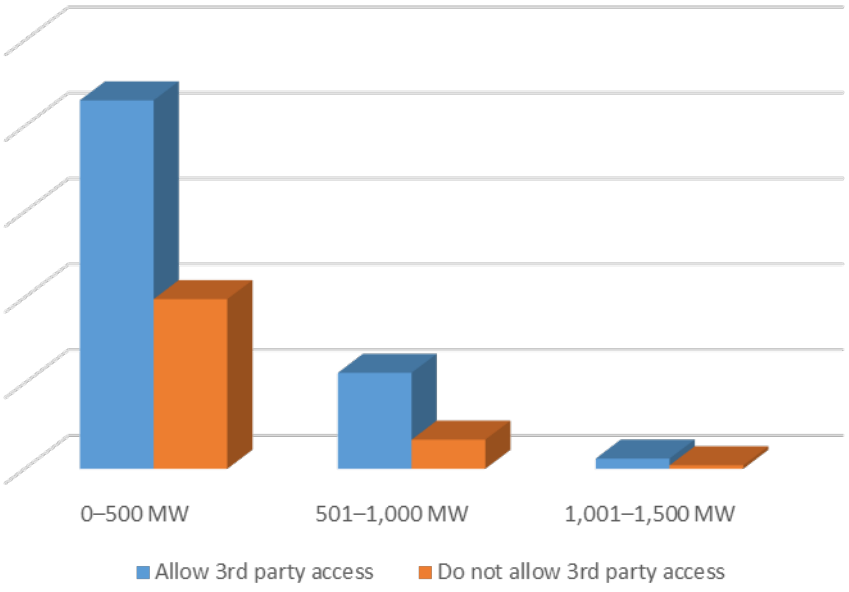


Figure 2.9: Generation Resources for Entities with only Low Impact BES Cyber Systems

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.

MEMORANDUM

TO: Roy Thilly, Chair
NERC Board of Trustees

FROM: Jack Cashin, Director, Policy Analysis and Reliability Standards, American Public Power Association
John Di Stasio, President, Large Public Power Council
John Twitty, Executive Director, Transmission Access Policy Study Group

DATE: January 22, 2020

SUBJECT: Response to Request for Policy Input to NERC Board of Trustees

---

The American Public Power Association, Large Public Power Council, and Transmission Access Policy Study Group concur with the Policy Input submitted today by the State/Municipal and Transmission Dependent Utility Sectors of the Member Representatives Committee, in response to NERC Board Chair Roy Thilly's January 2, 2020 letter requesting policy input in advance of the February, 2020 NERC Board of Trustees' meeting.

NERC Board of Trustees Policy Input – Canadian Electricity Association

The Canadian Electricity Association ("CEA") appreciates this opportunity to provide further policy input to the NERC Member Representatives Committee ("MRC") and Board of Trustees ("Board").

Summary of Key Points:

- CEA appreciates the work of the EMP Task Force, and the opportunity for industry to provide input on this complex issue.
- CEA urges NERC to recognize where EMP protection is beyond registered entity roles and, where actions are proposed, suggests that these take the form of a guideline or recommendation that can be adapted to NERC's members' national contexts.
- CEA is supportive of the proposed Supply Chain Risk Assessment modification and that the recommendation was based on NERC studies. CEA also appreciates NERC's clear and ongoing communication with member entities regarding this issue.
- CEA is supportive of the policy input letter comments submitted by Lloyd Linke in his role as representative of the Portion of Sector 4 representing the Federal Utilities and Federal Power Marketing Administrations.

Electromagnetic Pulse Strategic Recommendations

- CEA appreciates the work of the Electromagnetic Pulse ("EMP") Task Force, and the opportunity for industry to comment on this complex issue before further NERC work on EMP continues.
- As NERC pursues its work on EMP issues, CEA encourages NERC to consider whether integrating the EMP Task Force's scope of work into an existing Task Force or Working Group could provide efficiencies.
- As any further action is taken on EMP issues, CEA would urge that NERC recognize where EMP threat mitigation and protection actions and issues are under the purview of government authorities.
    - Given the nature of any EMP threats, EMP protection may be beyond registered entity roles, and the task force should be cognizant of this in any recommendations they make.
    - Any NERC activities should also complement or leverage existing activities by governmental or other relevant stakeholder groups.
    - CEA would support NERC efforts to develop a framework for ongoing consultation and dialogue between governments from both Canada and the U.S., supported by industry participation.

- CEA would caution against action towards a proposal of a standard for protection, control, and/or communication infrastructure that mandates 'military style' hardening, as utilities may struggle to implement it. CEA instead recommends the development of guidelines or recommendations.

    - Consideration will also be needed for any differences in perspectives and applicability of any suggested EMP mitigation or protection measures between the U.S and Canada. Proposed actions should be adapted to the national context and the priorities of respective governments.

    - Should a standard be developed, the standard development process should include consideration of the unique Canadian landscape and jurisdictional realities, including flexibility that may be required in implementation, as has been used in other standard development processes.

    - Furthermore, CEA notes that cost recovery may be a concern for any new standards, potentially entailing hardening beyond what is currently scoped in the CIP-014 and GMD standards, as well as funding outside of the usual ratepayer cost recovery mechanisms.

- As any work on EMP issues proceeds, it will be fundamental to consider both Canadian and U.S. perspectives on EMP planning, mitigation and recovery.

Supply Chain Risk Assessment

- CEA is supportive of the recommendation to modify the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity and would support the applicability of the CIP-013 standard to all equipment likely to be subject to CIP standards.

    - Furthermore, protected cyber assets ("PCA") and transient cyber assets/removable media ("TCAs/RM") should be protected against supply chain cyber security risks.

- CEA members appreciate the clear and ongoing communication by NERC regarding its supply chain activities, and its efforts to ensure affected entities were aware of the possibility of this proposed modification.

    - This communication has served to increase industry readiness.

- As cyber security supply chain risks can be complex, CEA appreciates that this recommendation was made based on the conclusions of NERC studies.

    - This serves to increase confidence that this recommendation is based on a measured and thoughtful approach.

- While CEA is supportive of the recommendation, CEA appreciates NERC's efforts to ensure supply chain risks are fully addressed in the most efficient manner by providing the opportunity for comment on if there an alternate way to address the identified risk in a more cost-effective manner.

- It has been noted that for some CEA members, that the recommended path is efficient and will be minimally burdensome as they treat low impact systems in generally similar ways to medium impact ones.

CEA thanks the Board for considering these comments. CEA and its members look forward to continuing the discussion going forward.

Dated: January 22nd, 2020

Contact:
Francis Bradley
President & CEO
Canadian Electricity Association
Bradley@electricity.ca

Edison Electric INSTITUTE

Power by Association

Policy Input for the NERC Board of Trustees Provided by the Edison Electric Institute January 22, 2020

On behalf of our member companies, the Edison Electric Institute (EEI) appreciates the opportunity to provide the following policy input for the NERC Board to review in advance of the meetings in Manhattan Beach, CA. EEI perspectives on bulk-power system (BPS) reliability are formed by our CEO Policy Committee on Reliability, Security, and Business Continuity and the Reliability Executive Advisory Committee with the support of the Reliability Committee.

In the January 2, 2020 policy input letter, NERC Board of Trustees Chair, Roy Thilly, seeks input on the Electromagnetic Pulse Strategic Recommendations (EMP Report) and Supply Chain Risk Assessment recommendations. EEI offers the following input.

Summary of Comments

Item 1: Electromagnetic Pulse Strategic Recommendations

- Focus efforts on addressing BPS risk in light of December 20, 2019 federal law imposing requirements on federal agencies regarding coordination of response and recovery and revisit the recommendations accordingly.
- EEI generally supports priority of recommendations but some adjustments within specific recommendations is warranted.
- Ensure uniformity of recommendations with policy input letter.

Item 2: Supply Chain Risk Assessment

- Risk conclusions need more thorough technical support and detailed explanation.
- Gather information from implementation of medium and high assets to determine lessons learned and an approach for evaluating treatment of low assets.
- Consider whether and where in the current framework of standards treatment of low assets could reside.

Item 1: Electromagnetic Pulse Strategic Recommendations

Electromagnetic Pulse (EMP) is a high priority for the United States government as demonstrated in the recent enactment of the National Defense Authorization Act (2020 NDAA) which codified in large part the Presidential EMP Executive Order – March 2019. Many federal agencies, notably the Federal Emergency Management Agency (FEMA) have authority to coordinate responses to and recovery from EMP attacks. That said, the EMP Strategic Recommendations (EMP Recommendations) may need to be revisited in light of this new law. With respect to the specific recommendations, many echo the recommendations made and actions taken by other organizations. Several other industry and governmental organizations (e.g., DOE, EEI, EPRI, NATF) have produced reports and initiated actions to address EMP threats. As NERC recognizes in the recommendations, timing and sequencing of the recommendations is crucial. Consequently, EEI recommends that the EMP Recommendations be reviewed to ensure they align with the government agencies and other organizations in recognition of those activities that are underway, or otherwise identified, in the 2020 NDAA.

In particular, the EMP Recommendations appear to address both policy and reliability items that will be led by government agencies under the NDAA. For this reason, we suggest that NERC focus industry efforts on those activities within the EMP Recommendations that address the risks to the BPS and are not appropriate for other organizations to be leading.

In addition, some of the recommendations in the policy input letter are worded differently from the EMP Recommendations. NERC should ensure the language is consistent or explain why the wording was changed.

EEI generally agrees with the priorities shown in bold in the EMP Recommendations but notes that additional prioritization within the specific recommendations is necessary because certain recommendations depend on the completion of other activities. EEI suggests the following for the identified Recommendations.

<u>Policy Priorities</u>

1. Recommendation #1: BPS Performance Expectations for an EMP Event - EEI agrees with the prioritization.
2. Recommendation #3 - Coordination with Other Sectors - EEI suggests this recommendation is a policy matter and should be undertaken by organizations with the appropriate policy expertise. While other entities may be better positioned than NERC to address and drive coordination efforts toward enhancing EMP resilience nationwide, it is important for NERC to emphasize the critical interdependencies of these other sectors with the BPS. For these reasons, NERC and the EMP Task Force should act as a support organization for efforts to address interdependencies.

3. Recommendation #2 - Industry & Public Education - EEI supports NERC's involvement in developing educational material about EMP but does not support its involvement in providing this material for "other interested parties" or the "general public." EEI suggests removing "Public" from this Policy Recommendation to better focus on BPS reliability and those activities needed to support industry.

Research & Development Priorities

1. Recommendation #2: Identify Gaps in Research - EEI agrees that the ERO Enterprise should support efforts to close existing knowledge gaps that might impact the reliable operation of the BPS and the prioritization recommended. However, because this recommendation includes distribution systems, NERC should be mindful of its limitations with respect to local distribution as it seeks to close knowledge gaps. Collaboration with industry and key research partners is crucial.
2. Recommendation #3: Develop Industry Specifications for Equipment - EEI supports the revised scope for this activity in the policy input as compared to the scope described within the EMP Task Force Strategic Recommendations (Research Recommendation #3), which indicate that the IEEE and NERC should co-lead efforts to develop equipment design specifications for the electric sector. EEI supports NERC and the EMP Task Force participation in the process and NERC efforts to communicate the various activities to industry throughout the process.
3. Recommendation #1: Monitor Current Research and Report on National Initiatives – EEI supports the prioritization recommended.

Vulnerability Assessment Priorities

It may be necessary to address some of the policy and research and development priorities prior to engaging in the vulnerability priorities. EEI requests clarification regarding the omission of Recommendation #1: Collaboration and Coordination with Federal Government.

1. Recommendation #2: EMP Vulnerability Assessments Methods - While EEI supports any effort to improve the industry's ability to assess reliability risks to the BPS, we are also concerned that any effort to effectively accomplish this task is tied to "access to unclassified EMP environments", which have not yet been released. Moreover, NERC may want to consider that any public disclosure of industry efforts to protect the grid from EMP exposure might only serve to provide adversaries with an understanding of how to launch an effective attack on the grid.
2. Recommendation #3: Critical Assets Identification - EEI agrees with the prioritization.

Mitigation Guideline Priorities

1. Recommendation #1: Develop Guidance on EMP Mitigation - EEI agrees with the lower prioritization of this recommendation. This topic could be addressed in parallel with other efforts when information is made available. This may provide opportunities to drive lower-cost solutions that could benefit both reliability and resiliency.

Response & Recovery Priorities

1. EEI agrees with the prioritization of these recommendations.

Item 2: Supply Chain Risk Assessment

It is critical to identify and find solutions to the cyber security risks to the BES, but additional research, analysis and considerations of existing CIP Standards need to be conducted prior to accepting the recommendation to modify the supply chain standards. For many years, NERC's focus has been on a risk-based approach to grid reliability, and the CIP Standards, including the Supply Chain Standard, were developed with that in mind and appropriately focus on higher risks to reliability.

The Risk Assessment needs additional clarity on the nature of the risk and a more robust technical analysis to support and understand the conclusions that the supply chain requirements address the identified risk. Some conclusions are presented on what appear to be arithmetical computations and lack a technical analysis and explanation on the nature of the risk of low impact assets. As an example, the Risk Assessment concludes that a small percentage of local transmission and substation assets could in the aggregate have an impact on BES reliability beyond the local area, but there is no explanation of how this conclusion was reached. Specifically, NERC notes that "[a]n individual compromise to any one of these locations (transmission station and substation or generation resource) would generally be a localized event." Therefore, a common mode vulnerability affecting numerous low impact BES Cyber Systems through their external routable connectivity appears to be the only risk identified.

The electronic access controls for lows in Reliability Standard CIP-003-7, Attachment 1 are a direct response to NERC's proposed method of countering coordinated cyberattack by restricting third-party electronic access to low impact locations. To the extent a technical analysis supports the need for additional protection for the connectively of low assets, such protection would reside in Reliability Standard CIP-003.

Additionally, more analysis, explanation, and research are also needed to understand whether the recommendation to include low impact BES assets with external routable connectivity in the supply chain standards is appropriate. To better inform an analysis of low assets, NERC should consider delaying this effort until it can gather additional information on how entities are implementing the standards for medium and high assets. The industry is in the process of addressing

medium and high assets with a July 2020 deadline for compliance with CIP-013-1. It would be premature and could have unintended effects without first understanding the impact and treatment of medium and high assets to determine an appropriate approach for low assets.

With a more thorough technical analysis, EEI would be better equipped to evaluate the conclusions of the Risk Assessment, which would allow a productive dialogue of how to best treat low impact assets in the framework of a risk-based approach. As part of this additional analysis, it is important for NERC to gather information from the implementation of the soon to be effective CIP Standards.

Thank you for the opportunity to provide policy input.

Sector 8 Policy Input for the NERC Board of Trustees & Member Representatives Committee

February 5-6, 2020 Meetings in Manhattan Beach, CA

ELCON, on behalf of Large End-Use Consumers, submits the following policy input for the consideration of NERC's Board of Trustees (BOT) and the Member Representatives Committee (MRC). It responds to BOT Chairman Roy Thilly's January 2, 2020 letter to Greg Ford, chair of the MRC.

SUMMARY

- **Item 1: Electromagnetic Pulse Strategic Recommendations**—ELCON supports the recommendations and proposed priority levels.
- **Item 2: Supply Chain Risk Assessment**—ELCON disagrees with NERC's recommendation that the Supply Chain Standards be revised to include low impact BES Cyber Systems with remote electronic access connectivity. We believe the analysis as presented by NERC does not represent a supply chain risk but rather a remote access control risk. Allowing necessary connectivity does not inherently increase an entity's supply chain risk. Access controls are in place on these low impact BES Cyber Systems based on the requirements of CIP-003. ELCON believes there are more cost-effective methods in which to address the true risk identified in NERC's analysis. Modifications to CIP-003 Electronic Access Controls could provide additional risk mitigation in a more cost-effective manner. And any modifications should follow the current CIP model so that any requirements applicable to low impact BES Cyber Systems remain in CIP-003.

Item 1: Electromagnetic Pulse Strategic Recommendations

Protecting the bulk power system (BPS) and achieving effective reduction of reliability risk is integral to the Electric Reliability Organization mission. Recognizing the risk potential from electromagnetic pulses (EMPs), NERC launched an effort to better understand reliability concerns associated with EMPs and to identify ways to enhance resilience in the face of these concerns. NERC created the EMP task force in April 2019 to identify key issues and scope opportunities for action. At its November 2019 meeting, the board accepted the EMP task force's report that included a series of strategic recommendations. Recognizing the broad expanse of the recommendations in the report and NERC's focus on effectiveness and efficiency, the board

asked NERC staff to propose which recommendations should be pursued first and EMP priorities for the ERO Enterprise for the long term. In response, NERC staff is recommending that the EMP Task Force should be maintained and serve under the new Reliability and Security Technical Committee (RSTC) with a specific workplan. NERC staff also proposes the following priorities for addressing the other recommendations in the report. Each section is provided in prioritized order. Items that NERC staff has identified as the highest overall priority, and thus should be addressed in the near term, are provided in bold.

Policy priorities:

1. The EMP Task Force should establish performance expectations for the BPS regarding a predefined EMP event. NERC staff will work with other agencies on areas that require coordination.

2. The EMP Task Force should develop guidance for the electric industry on interdependent utility sector coordination related to an EMP event.

3. The ERO Enterprise should develop educational materials about EMPs and their impact to electronic devices and BPS stability to inform industry and other interested parties.

Research and Development priorities:

1. The ERO Enterprise should support additional research to close existing knowledge gaps into the complete impact of an EMP event to understand vulnerabilities, develop mitigation strategies, and plan response and recovery efforts.

2. The EMP Task Force should work with other standards setting organizations (e.g. IEEE, Underwriters Laboratories) to designate equipment specifications for the electric sector utility industry around EMP hardening and mitigation strategies.

3. The ERO Enterprise should monitor and communicate to the industry research pertaining to EMP and EMP-related national security initiatives that impact the BPS.

Vulnerability Assessments priorities:

1. The ERO Enterprise should develop tools and methods for system planners and equipment owners to use in assessing EMP impacts on the BPS.

2. The EMP Task Force should provide guidance to industry on how to identify and prioritize hardening of assets that are needed to maintain and restore critical BPS operations.

Mitigation Guideline priorities:

1. The EMP Task Force should develop guidelines for industry to use in developing strategies for mitigating the effects of an EMP on the BPS (control centers/plant controls, substations, and power plants).

Response and Recovery priorities:

1. The EMP Task Force should develop guidance for supporting systems and equipment (including spare equipment strategy) needed for BPS recovery in a post-EMP event.

2. The EMP Task Force should develop response planning guidelines for EMP event pre- and post-contingency actions that aligns with plans of applicable regulatory authorities.

3. The EMP Task Force should develop criteria to incorporate into operating plans and procedures and system restoration plan actions pertaining to EMP event.

4. The RSTC should develop training for system and plant operators about EMP events and consider incorporating EMP events in coordinated industry exercises to test response planning and system restoration recovery efforts.

5. The ERO Enterprise should work with the appropriate agencies to develop a real-time national notification system for the electric sector to System Operators and Plant Operators pertaining to an EMP event and its parameters.

The ERO Enterprise will facilitate conversations with appropriate agencies to encourage the development of solutions to the following policy matters outside of its scope:

- Cost recovery mechanisms for planning, mitigation, and recovery plans required to be developed.

- Access to necessary research by key industry personnel with security clearances (at the appropriate levels) conducted by the National Labs, Defense Threat Reduction Agency, and any additional third-party research on electric utility equipment by the Department of Energy.

- Access to industry-relevant information on E1, E2, and E3 EMP environments and other necessary related research.

The BOT requests MRC policy input on the following:

1. Do you agree with the recommendations above?

2. Do you agree with the priority levels proposed by NERC staff to address the recommendations?

3. Are there any additional recommendations related to EMP that the Board should consider?

ELCON Response:

ELCON supports the recommendations and proposed priority levels.

Item 2: Supply Chain Risk Assessment

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.

Based on the analysis of the data request outlined in the Supply Chain Risk Assessment (Attachment B), NERC staff is recommending modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity.

1. Do you agree with the recommendation?

ELCON Response: We appreciate NERC's efforts to help mitigate cyber security risks associated with the supply chain. We however disagree with NERC's recommendation that the Supply Chain Standards be revised to include low impact BES Cyber Systems with remote electronic access connectivity. The recommendation is based on the data NERC collected from registered entities pursuant to the Section 1600 data request issued on August 15, 2019 and NERC's analysis of that data. We believe the analysis as presented by NERC does not represent a supply chain risk but rather a remote access control risk. NERC's analysis and recommendation focused on entities that "allow" inbound and outbound connectivity but the question and therefore the analysis doesn't go far enough to determine what an entity actually means when it "allows" inbound and outbound connectivity. Attachment 1 of CIP-003 requires entities to implement electronic access controls that permit only necessary inbound and outbound electronic assess between low impact BES Cyber Systems and Cyber Assets outside the asset containing low impact BES Cyber Systems. Allowing necessary connectivity does not inherently increase an entity's supply chain risk. Access controls are in place on these low impact BES Cyber Systems based on the requirements of CIP-003. Currently all CIP requirements applicable to low impact entities reside in CIP-003 and the protections required under CIP-003 allow an entity to apply the protections at the asset level. CIP-013, CIP-010 and CIP-005 are not structured to allow an entity to apply controls at an asset level and therefore would require a major overhaul to include low impact BES Cyber Assets/Systems. Requiring an analysis of every low impact BES Cyber Asset/System and implementing supply chain controls on them would result in significant

costs with little to no risk benefit. Such an overhaul is in direct conflict with the current CIP standards model and industry would bear considerable cost to change that model for little risk benefit. Additionally, the supply chain requirements under CIP-013, CIP-010 and CIP-005 have not yet been fully implemented. A complete overhaul of those standards seems premature until implementation is further along.

2. Is there an alternate way to address the identified risk in a more cost-effective manner?

ELCON Response—We do believe there are more cost-effective methods in which to address the true risk identified in NERC's analysis. NERC's report highlighted its concern that low impact BES Cyber Systems that allow remote access pose a significant risk of a coordinated cyberattack. Modifications to CIP-003 Electronic Access Controls could provide additional risk mitigation in a more cost-effective manner. Ultimately the focus of any standards modification should be focused on connectivity as opposed to supply chain in order to address NERC's concern of a coordinated cyberattack. And any modifications should follow the current CIP model so that any requirements applicable to low impact BES Cyber Systems remain in CIP-003.

###

TO: Roy Thilly, Chair
NERC Board of Trustees

FROM: Lloyd A, Linke
Federal Utility/Federal PMA Portion Sector 4

DATE: January 22, 2020

SUBJECT: Response to Request for Policy Input to NERC Board of Trustees

The Portion of Sector 4 representing the Federal Utilities and Federal Power Marketing Administrations (Federal PMA), appreciate the opportunity to respond to your January 2, 2020 letter to Mr. Greg Ford, Chair NERC Member Representative Committee, requesting input on certain policy issues. The Federal PMA appreciates the opportunity to provide comments on the policy input on two matters of particular interest to the NERC Board of Trustees (Board) for their Feb. 5-6, 2020 meeting. We offer the following on Electromagnetic Pulse Strategic Recommendations and on Supply Chain Risk Assessment.

The Federal PMA is in support of NERC staff recommendation to maintain the EMP Task Force and it would be best to have it serve under the new Reliability and Security Technical Committee (RSTC) with a specific work plan.

Electromagnetic Pulse Strategic Recommendations

The following are more specific responses to questions asked by the NERC BOT on the Policy Input Letter on the EMP;

1. **Do you agree with the recommendations above?**

   The Federal PMA agrees with Staff recommendations as outlined, recognizing that they are general and wide-ranging; likely glossing over the complexities of who has the primary obligation to protect against EMP versus what shall be the expectations for transmission system performance following an EMP. The recommendations represent merely the beginning of the beginning. Countless technical details, including quantifying the basics of the EMP event risk itself, remain to be determined.

2. **Do you agree with the priority levels proposed by NERC staff to address the recommendations?**

   The Federal PMA agrees with Staff priority levels.

3. **Are there any additional recommendations related to EMP that the Board should consider?**

   a. We recommend that the task force consider the vulnerability of an electric utility's microwave and fiber communication system due to an EMP event,

b. The Federal PMA would like Staff to consider to expand EMP impacts to **fleet utilities** used for operation and maintenance of BPS. This addition would impact each of the areas identified above. Current fleets are mostly dependent on electronics and ran by computer. Newer fleets might have EMP protections but not all fleets do have such protection.

c. We expect that once the recommendations are accepted, the first task force efforts will center around defining the EMP event of interest which directly affect the practical implications of Research Recommendation #3 (Develop Industry Specifications for Equipment), as well as the related Vulnerability Assessment Recommendation #2 (EMP Vulnerability Assessment Method).

d. Economic consideration and cost impact and cost recovery are factors that should be considered in all the mitigation strategies**.**

Supply Chain Risk Assessment

The following are more specific responses to questions asked by the NERC BOT on the Policy Input Letter on the Supply Chain Risk Assessment report dated Dec. 9, 2019;

1. **Do you agree with the recommendations above?**
    a. The Federal PMA is in support of the recommendations outlined in the Supply Chain Risk Assessment Analysis of Data Collected under the NERC Rules of Procedures Section 1600 data Request dated Dec. 9, 2019 report.
2. **Is there an alternate way to address the identified risk in a more cost effective manner?**
    a. The Federal PMA recommend that NERC investigate the creation of a supply chain certification program for vendors.
    b. Further assessment by each entity is needed to access that economic impact. As Staff noted many of large entities already factor in the low facilities as part of their procurement policies and standards. Concerns lies on smaller utilities with much lower budget and their ability to deal with supply chain standards.
    c. The third party access to either low only transmission systems or to the generation sites could be problematic. The Federal PMA suggests further coordination with those entities that use third party access to have monitoring and controls in place to limit the exposure of impact on the BPS system.

The Federal PMA support the comments provided by the Canadian Utilities in Sector 4.

Policy Input to the NERC Board of Trustees
February 6, 2020, Manhattan Beach, CA
Provided by the North American Generator Forum

The North American Generator Forum appreciates the opportunity to provide the following policy input in advance of the NERC BOT meeting.

Summary

Item 1: Electromagnetic Pulse Strategic Recommendations

The NAGF appreciates the opportunity to provide policy input for the NERC Member Representatives Committee ("MRC") and Board of Trustees ("Board") in response to Mr. Greg Ford's letter dated January 2, 2020. Overall, the NAGF supports the EMP recommendations. The NAGF identifies some adjustments regarding the proposed priority levels and additional recommendations related to EMP for consideration.

Item 2: Supply Chain Risk Assessment

The NAGF appreciates the opportunity to provide policy input for the NERC Member Representatives Committee ("MRC") and Board of Trustees ("Board") in response to Mr. Greg Ford's letter dated January 2, 2020. The NAGF does not agree with the recommendation of modifying the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. The NAGF provides alternative methods for consideration for addressing the identified risk in a more cost effective manner.

Discussion

Item 1: Electromagnetic Pulse Strategic Recommendations

The Board requests MRC policy input on the following:

1. Do you agree with the recommendations?

Policy – The NAGF agrees with the recommendations.

Research and Development – The NAGF agrees with the recommendations. Consider using a tiered approach for development of vulnerability understanding, mitigation strategies, and response/mitigation efforts.

Vulnerability Assessments - The NAGF agrees with the recommendations. Consider moving Recommendation #2 under the Mitigation Guideline section.

Mitigation Guideline – Consider combining Recommendation #1 with Vulnerability Assessments Recommendation #2.

Response and Recovery - The NAGF agrees with the recommendations.

2. Do you agree with the priority levels proposed by NERC staff to address the recommendations?

The NAGF agrees with the priority levels proposed for Policy, Research and Development, and Vulnerability Assessments. Consolidation of Mitigation Guideline Recommendation #1 and Vulnerability Assessment #2 would justify a higher priority for the resulting recommendation. The NAGF recommends that Response and Recovery Recommendation #5 be given a higher priority.

3. Are there any additional recommendations related to EMP that the Board should consider?

The NAGF recommends development of a clear EMP event definition and associated performance expectations which are necessary for industry to support EMP resilience. EMP event communication guidelines will provide important event details for industry thus enabling the appropriate and safe response to an EMP event. Cost recovery mechanisms need to be developed to fully/partially offset the cost associated with securing critical infrastructure for EMP events. Note that the Nuclear GO/GOPs will be submitting separate comments through the Nuclear Energy Institute (NEI) to address their specific concerns related to the EMP task force's recommendations.

Item 2: Supply Chain Risk Assessment

The Board requests MRC policy input on the following:

1. Do you agree with the recommendation?

The NAGF does not agree with the recommendation of "modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity". We believe the data in the assessment suggests that this is not a supply chain risk, but rather a connectivity/remote access risk.

We agree that the current CIP standards have appropriately considered each individual generating resource having a low impact to the BES. We also agree with the model outlined in CIP-002 that treats such generating sites at an ‘asset' level and protecting the site as one ‘asset containing lows' rather than at an individual cyber asset level due to their low impact and very large scale.

Our concern is that the recommendation conflicts with the CIP Standards model that is currently in place that does not require an inventory of BES Cyber Assets for lows (CIP-002), and where all security requirements for lows are contained in CIP-003. The CIP-005, CIP-010, CIP-013 supply chain standards were not designed for the "asset containing lows" model but rather for the high/medium impact cyber asset/system level model. Analyzing every cyber asset within generating facilities in order to put the CIP-005, CIP-010, CIP-013 controls in place upends the enormous efforts and costs utilities have put forth to implement security and compliance programs to meet the current suite of CIP Standards, and does little if anything to address risk identified in the assessment.

It should also be noted that the Supply Chain Standards for high/medium impact systems have not been implemented and expanding the scope to include the significantly more extensive low impact systems does not appear prudent at this time.

Instead, we believe there are alternate ways to mitigate the identified risk that do not break the current CIP Standards model and that would be targeted to the address the risk identified in the assessment.

2. Is there an alternate way to address the identified risk in a more cost effective manner?

The NAGF believes there are alternatives to address the identified risk, not only in a more cost-effective manner, but in ways that build on the CIP-002 and CIP-003 models already in place.

The current CIP-003 Electronic Access Controls for low impact are a good first step and this approach should be leveraged to build on the processes already in place that address this risk. The risk of a coordinated attack over external connectivity and remote access would more holistically be addressed by Electronic Access Controls rather than just the vendor slice of it or by invoking an fundamental change in the CIP-002 low impact strategy resulting in a ‘do-over' of the standards.

We believe that remote access protections that build on existing CIP-003 protections for lows would provide a greater risk reduction. It is preferred that recommendations for improving remote access protections not be technology specific and applicable to only solutions used or available at the point-in-time of issuance of any new directives. Specific protections often prevent better solutions from being applied and prevent retirement of approaches that are no longer effective or best-in-class. This is particularly true for cyber protections and the fast-moving technology that it incorporates.

For example, requiring protections such as intrusion detection/prevention, multi-factor authentication, or remote access session management in a general sense and allowing entities to specify and justify their approaches around implementation would better serve the industry. Having flexibility in deploying these options can improve security as well as provide a ‘standard’ means of protection that can reduce the vulnerability of a system. Enhancements to the current CIP-003 Electronic Access Controls section would maintain the existing low impact framework and still function at an "asset containing lows" level.

We believe the suggested approach to be more cost-effective because it allows the focus to be on effective centralized security controls on the external connectivity and ALL remote access rather than on a massive and costly effort without a corresponding level of benefit. It is far more cost effective to focus on the entry points and requiring stronger technical controls on remote access, along with the newly required controls on Transient Cyber Assets and Removable Media, which focuses our resources on those entry points and provides the most "bang for the buck" in protecting ALL BES cyber systems within a generating resource.

We request that any new directives focus on the risk to be addressed, and not delve into what to put in what particular standard. We will get a better solution if that is left up to the SAR and SDT process to determine with industry input where and how to best address the risk in the suite of CIP Standards in ways that can mitigate the risk in our unique situations without breaking all of our existing security and compliance programs built on the current CIP model.

In a nutshell, if the risk is a coordinated attack using the large amount of external connectivity to low sites, then let's focus on putting controls to protect that connectivity and ALL users and sessions that use it.

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

To: NERC Board of Trustees (BOT)

From: Thomas J. Galloway, NATF President and CEO

Date: January 20, 2020

Subject: NATF Policy Input to the NERC BOT (February 2020): EMP Strategic Recommendations

The North American Transmission Forum (the "NATF") appreciates the opportunity to provide policy input on electromagnetic pulse (EMP) strategic recommendations.

Summary Input

NATF's policy input remains consistent with the input previously provided informally to NERC staff and the EMP Task Force. Specifically:

- Implementation of EMP recommendations needs to proceed in a disciplined and methodical manner, with careful consideration of proper sequencing
- EMP recommendations should be implemented holistically with respect to resiliency overall, not narrowly through an EMP-centric lens
- NERC can serve a useful convening and organizing function but should make full use of the work that has already been completed or is underway

Full Input

Policy Priorities

Policy priority #1 indicates that the EMP Task Force should establish performance expectations for the BPS regarding a predefined EMP event. Significant work remains to characterize the nature of threat, determine system impact, and develop mitigations. As suggested in our previous input, we believe that this work is best approached via a disciplined framework that considers prerequisites.

Policy priority #2 indicates the EMP Task Force should develop guidance for the electric industry on interdependent utility sector coordination related to an EMP event. Significant work on this front has already been completed or is under development by the Electric Subsector Coordinating Council (ESCC) and the NATF (e.g., grid security emergencies). Those activities should be reviewed in detail and leveraged before developing new guidance.

Similarly, policy priority #3 indicates the ERO should develop educational materials about EMP and related impacts. The Electric Power Research Institute (EPRI) has an extensive body of research and educational materials that could be leveraged in this area.

Vulnerability Assessments and Mitigation Guidelines

EPRI and the NATF can both contribute significantly on vulnerability assessments and related mitigation practices. There is already a body of established work and ongoing activities on both these fronts.

Response and Recovery

EMP is one of the four initiating event types for the declaration of a grid security emergency. The ESCC, NATF, Department of Energy, and trade organizations have been actively engaged on this front for about two years. It would be important to leverage that work to help reduce the potential for misalignment or duplicative effort.

cc: NATF Board: E. Seidler, J. Bladow
NATF Staff: Keels, Carter, Aldred, Underwood

NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Policy Input
From a Northeastern North American Reliability Perspective
By the NPCC Board of Directors

1. Electromagnetic Pulse Strategic Recommendations

- The NPCC Board supports the priority levels proposed to address the EMP Report recommendations.
- The NPCC Board also supports continuation of the subject matter expert EMP Task Force working to develop recommendations for performance expectations for the bulk power system for an EMP event, under the strategic policy direction of the stakeholder-balanced Reliability and Security Technical Committee.
- The NPCC Board recommends that, in addition to supporting additional research into the impacts of an EMP event, the ERO Enterprise work closely with government agencies, industry stakeholders and policy makers to facilitate agreement on parameters associated with a predefined EMP event, with special attention to E3 events.
- The NPCC Board also recommends that the potential impacts on the BPS of the performance of sophisticated electronics associated with distributed energy resources and battery management systems for an EMP event be included in the EMP Task Force's considerations.

2. Supply Chain Risk Assessment

- The NPCC Board supports the recommendation that low impact BES Cyber Systems with remote electronic access connectivity be considered in future modifications of the Supply Chain Standards.
- The NPCC Board recommends that cost effective protection alternatives for low impact BES Cyber Systems with remote electronic access connectivity be identified through the standard development process.

Affirmed by the NPCC Board of Directors
January 21, 2020
For submittal to the February 5-6, 2020
NERC MRC and BOT Meetings

JENNIFER L. UHLE
Vice President, Generation and Suppliers

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8164
jlu@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

January 22, 2020

Ms. Kristin Iwanechko
NERC
Suite 600, North Tower
3353 Peachtree Road NE
Atlanta, GA 30326

Subject: Electromagnetic Pulse (EMP) Strategic Recommendations [January 2, 2020]

Project Number: 689

Dear Ms. Iwanechko:

The Nuclear Energy Institute (NEI)[1], on behalf of its members and the NEI North American Electric Reliability Corporation (NERC) Issues Task Force (NITF), is pleased to respond to NERC's request for comment on the NERC EMP task force's recommendations as documented in the January 2, 2020 letter.

U.S. nuclear power plants are designed, built and maintained to safely withstand a wide variety of extreme events, including severe natural phenomenon. Nuclear safety systems are capable of withstanding the effects of an EMP due to the robust design of the nuclear plant structures and systems that would diffuse and attenuate the pulse. Following the events in Fukushima, Japan in 2011 the United States nuclear fleet added additional layers of protection called FLEX and SAFER. FLEX provides additional portable equipment deployed at each site to help respond to a nuclear emergency. To provide an additional level of safety, SAFER (Strategic Alliance for FLEX Emergency Response) Response Centers in Memphis and Phoenix were established and can deliver complete sets of emergency response equipment to any affected site within 24 hours after an extreme event.

Per the March 26, 2019, Executive Order on Coordinating National Resilience to Electromagnetic Pulses, Section 6, the Department of Homeland Security and the requisite Sector Specific Agencies (SSAs) must

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

identify any gaps in data regarding the effects of EMPs and address the gaps and vulnerabilities. The Nuclear Regulatory Commission (NRC) is coordinating with the DHS Cybersecurity and Infrastructure Security Agency (CISA) as the SSA for the commercial nuclear industry in completing the activities outlined in the Executive Order. The next deliverable for the NRC is the assessment of critical assets at nuclear facilities that are most vulnerable to the impact of an EMP, which is due in March 2020.

It should be noted that the NRC has evaluated potential EMP impacts on commercial nuclear power reactors and concluded that protection of the reactors and spent fuel pools during indefinite long-term loss of offsite power scenarios is the primary concern. Nuclear power plants maintain in excess of seven days of fuel oil on site but would require additional supplies for an indefinite period. On April 3, 2019 DHS CISA conducted a Fuel Supply Chain Coordination meeting to gather additional information to inform the National Risk Management Center's Fuel Logistics for nuclear power plants Under Regional ELAP[2] Conditions whitepaper.

All nuclear generating units are designed to automatically shut down on a loss of offsite power supply. Additionally, nuclear power plants are not permitted to startup if the local grid is not available. The EMP Task Force should recognize that, due to licensing and design requirements, nuclear generating units cannot be designated as a "Blackstart Resource" and should therefore be considered to be offline and unavailable until the grid is sufficiently recovered.[3]

The response to the specific Board questions is as follows:

1. Do you agree with the recommendations above[4]?

No.

Prioritizing the supply of diesel fuel oil to nuclear stations following an EMP event needs to be established as this ensures the affected nuclear reactors are maintained in a safe condition indefinitely.

Title 10 of the Code of Federal Regulation (CFR) Section 50.13 explicitly states, "…An applicant for a license to construct and operate a production or utilization facility, or for an amendment to such license, is not required to provide for design features or other measures for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other

[2] ELAP is an NRC acronym referring to an Extended Loss of AC Power.
[3] Provisions for considering the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power is contained in NERC Standard NUC-001-3, "Nuclear Plant Interface Coordination"
[4] The January 2, 2020 letter from the NERC board of trustees listed fourteen specific recommendations.

person, or (b) use or deployment of weapons incident to U.S. defense activities," consequently the NRC needs to evaluate such recommendations.

2. Do you agree with the priority levels proposed by NERC staff to address the recommendations?

No. First step should be resolving research and funding. The NRC is the Federal Regulatory Agency for civilian use of nuclear material and therefore any additional requirements posed on the industry would be issued by the NRC. However, EMP is an "enemy of the state" action and would not be the responsibility of the commercial nuclear industry. Consequently, cost for any upgrades would need to be incurred by the Federal government.

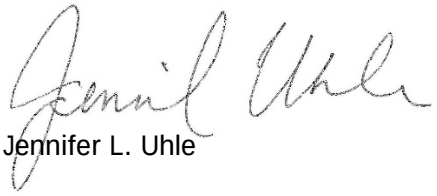
Preliminary timelines of when this project is expected to be completed would be beneficial.

3. Are there any additional recommendations related to EMP that the Board should consider?

Yes. The NRC and the regulated industry should be directly involved in the development of any recommendations that could impact commercial nuclear power plants.

If you have any questions, please contact Justin Wearne at jmw@nei.org or (202) 739-8087.

Sincerely,



Jennifer L. Uhle

c: Mark.Lombard@nrc.gov
Brian.Smith@nrc.gov

Cooperative Sector Policy Input to the NERC Board of Trustees
January 22, 2020

The Cooperative Sector appreciates the opportunity to provide policy input to the NERC Board of Trustees (BOT) for policy issues that will be discussed at the February 5/6 NERC MRC, Board, and Board Committee meetings.

Summary of Policy Input
The Cooperative Sector provides the following summary of its comments:

- *The Cooperative Sector supports the EMP Task Force's recommendations.*
- *The Cooperative Sector suggests that, because of the long-term and interdependent nature of several prioritized EMP Task Force recommendations, NERC reevaluate its proposed prioritization, giving due consideration to implementation time frame(s), interdependencies, and the need for coordination with and/or action by external parties, i.e., government agencies.*
- *The Cooperative Sector does not agree with the recommendation to include low impact BES Cyber Systems in the scope of applicability for reliability standard CIP-013-1. The data supporting the recommendation relies upon speculation and assumptions to support the identified risks.*
- *It is unclear to the Cooperative Sector whether the risk mitigation provided by the required security controls for low impact BES Cyber Systems was appropriately considered in overall risk identification.*
- *The Cooperative Sector recommends that additional data and information be collected and analyzed to ensure that identified risk(s) can be fully supported.*

Electromagnetic Pulse Strategic Recommendations

Question 1: Do you agree with the recommendations above?

- In the Cooperative Sector's opinion, the recommendations from the EMP Task force are sound and (once implemented) will achieve their goal of reducing reliability risk from EMPs. Accordingly, we support these recommendations and NERC's efforts to address and support industry and BES preparedness in the event of an EMP event. We also greatly appreciate NERC's recommendation to continue the EMP Task Force under the Reliability and Security Technical Committee (RSTC). This recommendation will allow important work to be sustained without interruption as NERC transitions the structure of its technical committees and working groups.

Question 2: Do you agree with the priority levels proposed by NERC staff to address the recommendations?

- While the Cooperative Sector agrees with the recommendations set forth in the EMP Report, we respectfully recommend that any prioritization of these recommendations should take into consideration the likely time frame for implementation of each recommendation as well as the potential to leverage and/or gain synergies during the implementation of dependent recommendations and through other, existing initiatives.
    - For example, the recommendation for the establishment of performance expectations appears to be a longer-term initiative that will require the prior completion of other recommendations, *e.g.*, information declassification and sharing; development of simulation tools, etc. More specifically, in order to set BES performance expectations, significantly more information regarding EMP events, their characteristics, and their effects on the BES will need to be determined, declassified,

shared, and evaluated. Hence, the implementation of the recommendation to establish performance expectations requires the prior, successful completion of other recommendations such as inter-agency and inter-entity information sharing and coordination and the development of additional assessment tools and methods.

- While the Cooperative Sector agrees that the establishment of performance expectations is a critical element of long-term preparedness for response to EMP events, we also respectfully assert that other recommendations, such as the development of guidance and educational materials, could provide more immediate value and benefit to the BES and the electric industry. For this reason, the Cooperative Sector recommends that NERC classify its priorities based on the time frame for completion and leverage the interim time periods associated with the implementation of longer-term or dependent recommendations to pursue recommendations that, while currently identified as lower priority, are more attainable in the near-term and would serve as stepping stones for the "higher" priority recommendations.
    - Regarding the prioritization of recommendations relative to EMP policy, the Cooperative Sector recommends that NERC prioritize the development of educational materials, and, then, utilize the knowledge and experience gained therefrom to develop guidance on coordination and other topics. The completion of these efforts in the near-term will not only benefit grid preparedness, but will also facilitate the implementation of more technical, longer-term recommendations, such as the establishment of performance expectations. This is especially true given that the successful establishment of performance obligations by the EMP Task Force is dependent upon the participation of experienced, knowledgeable industry stakeholders in the EMP Task Force and its activities.
    - Similarly, the prioritization of recommendations associated with research and development, vulnerability assessments, and response and recovery should be re-evaluated giving due consideration to time frames for implementation and the interdependency of the recommendations. In particular, for response and recovery, the prioritized recommendation is a long-term initiative that will require information and experience not currently available while the development of training and focused guidelines are shorter-term initiatives that could provide value to the BES and electric industry while the broader guidance is being developed.
- For these reasons, the Cooperative Sector respectfully recommends that NERC staff re-evaluate its prioritization giving due consideration to the concept that priorities should be identified for both the short- and longer-term time frames.

Question 3: Are there any additional recommendations related to EMP that the Board should consider?

- The Cooperative Sector appreciates the work of the task force and NERC staff for bringing awareness to several important, but out of scope, EMP-related issues. Additionally, the Cooperative sector notes that its review of the overall prioritization was impacted by a lack of clarity relative to certain recommendations identified as priorities. For example, how "performance expectations" is defined is unclear. As the NERC and the EMP Task Force continue to work on this important and evolving issue, additional clarity and industry outreach is recommended. The cooperative sector commends the ERO Enterprise for its continued leadership relative to the risk posed by EMP events to the reliability and security of the BES.

Supply Chain Risk Assessment

Question 1: Do you agree with the recommendation?

- The Cooperative Sector does not agree with this recommendation.
- The supply chain risk assessment gathered substantial data from industry; however, it is unclear whether the analysis of such data by NERC considered important characteristics that could have affected their determinations and recommendations.
    - For example, the analysis of data request responses performed by NERC and provided to the industry for input appears to rely heavily on assumptions that are not clearly correlated to or supported by the data collected. Such reliance, when due consideration is given to the tenuous nature of the data correlation, negatively impacts the credibility of the final determination and recommendation made by NERC.
    - In particular, the supply chain data request asked entities how their CIP-013-1, requirement R1 plan will affect low impact BES Cyber Systems and to describe the methods they intended to use to apply such plan to low impact BES Cyber Systems. This is an extremely narrowly-focused question that did not allow for entities to provide any insight or guidance into other security-related procurement strategies that they may be employing during the procurement of low impact BES Cyber Systems, *e.g.*, security-related contract provisions, third party risk reviews, chain of custody processes, etc.
    - For those entities that have existing security-related procurement strategies that are NOT the result of or directly derived from the entity's specific CIP-013-1, requirement R1 plan, the response to this question would have been negative. However, such response also would not necessarily have been representative of an entity's security risk mitigation strategies for low impact BES Cyber System procurement. Accordingly, the responses gathered, and assumptions made regarding such responses are insufficient to support a determination that low impact BES Cyber Systems are not subject to security risk mitigation strategies during their procurement.
    - Similarly, using only the number of asset locations, NERC determined that a coordinated cyber-attack with control of multiple low impact locations could result in an event that has an interconnection-wide BES reliability impact. However, the actual potential for such an impact is closely correlated with the geographic and electrical location of assets within an interconnection, their individualized, aggregate ability for impact within and beyond their local area, the overall electrical configuration within which such issue would arise, and other essential factors and characteristics. Neither number nor any of these additional factors alone are determinative of the likelihood or risk of an aggregate, interconnection-wide reliability impact. Hence, without additional context and evaluation of the low impact assets and their associated low impact BES Cyber Systems, the determination that sheer numbers of locations (regardless of location, size, electrical impact, etc.) would aggregate into an interconnection-wide impact cannot be supported and should not form the basis for the modification of the scope or applicability of a reliability standard.
    - Finally, the generalized nature of the third-party access question also does not provide enough information and context for the true risk and potential for impact to be discerned. The risk of third-party access cannot be evaluated in isolation - without an understanding of any processes, controls, or risk mitigation strategies being employed when such access is granted. Given the

right processes, controls, and risk mitigation strategies, granting a third-party access may not present any additional risk to the BES.

- For example, third party entities with access may be other registered electric industry entities with awareness of, and independent responsibility for, cyber security and reliability compliance. Additionally, an entity allowing third party access may have substantial and robust controls, such as background check requirements, continuous escorting, monitoring, or other protective measures. Further, while entities may allow third party access, criteria may be stringent; such access may be rare; and such access may have the effect of reducing risk and enhancing overall reliability. In particular, analysis must allow for the possibility that allowing third party access may, in certain circumstances, make available expertise, responsiveness, and resources that reduce risk and enhance overall reliability.
- Accordingly, *prima facie*, it appears arbitrary and unreasonable, without context and additional information, to definitively align the mere allowance of third-party access with significantly increased security risk. Because this finding of increased risk based on allowance of third-party access alone is clearly premature, it should not be relied upon as a basis for the modification of the scope or applicability of reliability standard CIP-013-1. Further, the Cooperative Sector notes that the current reliability standards for low impact BES Cyber Systems require that specific security controls be implemented to mitigate cyber security risk for these assets. It is unclear from the analysis provided whether NERC evaluated the effect of these required cyber security controls to determine their contribution to the mitigation of cyber security risk and the overall security of the BES.

- For these reasons, the Cooperative Sector does not, based on the information provided, agree with and cannot support the recommendation to include low impact BES Cyber Systems in the scope of applicability for reliability standard CIP-013-1.

Question 2: Is there an alternative way to address the identified risk in a more cost-effective manner?

- Because of the aforementioned concerns regarding the speculative nature of the identified risks and uncertainty regarding value ascribed to the mitigation provided by the existing security controls, the Cooperative Sector recommends that additional data and information be collected and analyzed to ensure that the identified risk(s) and associated recommendations can be fully supported and that any resulting scope expansions would be beneficial to reliability and cost-effective.
  - Specifically, the ERO should consider data including, but not limited to, the following: security-related procurement practices that are not derived from CIP-013, but that may be applied to a broader scope of assets; the reliability value and likely impact of low-impact assets for entities that have no high or medium impact assets; and ERO Enterprise observations following the implementation of the current supply chain standard.

Submitted on behalf of the Cooperative Sector by:
Barry Lawson
Senior Director, Regulatory Affairs
National Rural Electric Cooperative Association (NRECA)
703.907.5781
Barry.lawson@nreca.coop

NERC Board of Trustees

Manhattan Beach, CA
February 5-6, 2020
Policy Input of the Merchant Electricity Generator Sector

Sector 6, Merchant Electricity Generator Sector, takes this opportunity to provide policy input in advance of the upcoming North American Electric Reliability Corporation (NERC) Member Representatives Committee (MRC) and Board of Trustees (Board) meetings in Manhattan Beach, CA.

In a letter to MRC Chair Greg Ford dated January 2, 2020, Board Chair Roy Thilly requested MRC input on two items: Electromagnetic Pulse Recommendations and Supply Chain Risk Assessment Recommendations. Sector 6 makes the following comments in response.

Key Points

- The Merchant Generators generally support the Electromagnetic Pulse (EMP) Recommendations and priorities as listed knowing the priorities may well change in the future.
- The Merchant Generators do not fully agree with the recommendation to modify the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. We believe the data in the assessment supports the conclusion that this is a connectivity/remote access risk, not a supply chain risk. Enhancements to CIP-003 should mitigate this risk.

Sector 6 Comments for Policy Input

<u>Electromagnetic Pulse Strategic Recommendations</u>

The Merchant Electricity Generator Sector generally supports the Electromagnetic Pulse (EMP) Recommendations as listed. The effects of EMPs are still not well understood, and the recommendations provide a logical path to further research the issues and address impacts that are found. The Merchant Generators favor the EMP task force and NERC Staff's proposed approach of gathering additional needed information, running scenarios that impact the BES and the industry's capability to serve, interpreting results from those models, and providing guidance and education to the industry once the impacts and possible mitigations are identified.

We generally agree with the priority levels as proposed. We feel there may be a need for flexibility to change the priorities in the future if unforeseen impacts or vulnerabilities are identified that necessitate a change in overall approach. With so many players involved in the discussion we believe NERC needs to focus on the technical aspects of the EMP impacts, recovery, and mitigation.

The Merchant Generators have no additional recommendations to offer knowing that many social, political, financial and business issues will influence this topic for years to come. Being prepared with strong technical knowledge is the critical contribution that the ERO can add to the discussion.

Supply Chain Risk Assessment Recommendations

The Merchant Generators do not agree with the recommendation to modify the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. We believe the data in the assessment supports the conclusion that this is a connectivity/remote access risk, not a supply chain risk. The risks as noted in the assessment are real and we feel there is a more effective solution.

We support the comments and recommendations of the NAGF in their input on this matter and will not repeat them here. We believe that remote access protections that build on the existing CIP-003 requirements for low impact BES Cyber Systems would provide more effective risk reduction without upending current CIP implementation efforts and programs. The NAGF proposal allows for implementation flexibility, quick response to changing attacks, and addresses the issue directly.

Sincerely,
/s/
Sector 6 Merchant Electricity Generator Representatives:

Martin Sidor
NRG Energy, Inc.

Sean Cavote
PSEG

MEMORANDUM

TO: Roy Thilly, Chair NERC Board of Trustees

FROM: Jackie Roberts and Michael Moody – MRC Sector 9 Small End-Use Electricity Customer Representatives

DATE: January 22, 2020

SUBJECT: Small End-Use Sector (9) Response to Request for Policy Input to the NERC Board of Trustees

The representatives to the NERC Member Representatives Committee for the Small End-Use Customer Sector (9) appreciate the opportunity to provide these comments in response to the request in your letter to Mr. Greg Ford dated January 2, 2020.

Summary

Small End-Use Customer Sector (9) Sector 9 supports the EMP efforts to date. Small End-Use Customer Sector (9) notes improvement in planning and work plan development is needed. A precondition is collaboration with other regulatory and industry entities is needed to verify their support of the proposed plan before action can be implemented by NERC. In the comments below we elaborate on some points which we believe the BoT should consider regarding how to integrate EMP initiative.

Small End-Use Customer Sector (9) supports the Supply Chain efforts and Recommendation.

I. Electromagnetic Pulse (EMP) Initiative Strategic Recommendations

The Board requests MRC policy input on the proposed plans related to the EMP Initiative Strategic recommendations:

- Policy Priorities
- Research and Development Priorities
- Mitigation Guideline Priorities
- Response and Recovery Priorities
- Facilitation of conversations with appropriate agencies:

A. The NERC BoT asks whether Sector 9 agrees with the Electromagnetic Pulse Strategic Initiative Recommendations?

Yes. The Policy input letter identifies the recommendations and provides in bold print the NERC activities. Sector 9 agrees with the identification of the specific NERC activities within each recommendation area.

B. The NERC BoT asks whether Sector 9 agrees with the priority levels proposed by NERC staff to address the recommendations.

No, prioritization is premature in the context of the overall NERC business plan. It appears a ranking (1,2,3 etc.) within each recommendation area is provided to identify the relative position in time among the priorities. Sector 9 notes this ranking does not provide any guidance regarding the global priority within NERC for delivery of the work product(s) (e.g. guidelines and BPS performance expectations being the specific NERC deliverables) for which NERC is primarily responsible. This ranking does not provide any guidance regarding the time frame for delivery or resource intensity needed to create the various proposed work products. A specific timeline with milestones for each activity should be created to determine the incremental resource pressures that will be placed on NERC and the NERC stakeholders in light of many other NERC activities.

Currently, EMP risk is rolled into the cyber-security risk in the RISC risk mapping. Sector 9 believes that this may not be appropriate. The EMP risk may be a higher impact (emanating from a determined nation state foe), but a lower likelihood than cyber security attacks in general. This question regarding the EMP vs. cyber in general risk should be specifically answered (at least an industry consensus developed) before resources can be allocated to the EMP effort in the overall NERC plan. We note further that EMP is not specifically called out in the NERC Long-Term Strategic plan. Sector 9 agrees it is an emerging risk. This matter should be referred to the RISC for debate and characterization of the priorities.

C. The NERC BoT asks whether Sector 9 has any additional recommendations related to EMP that the Board should consider?

The NERC BoT should direct NERC staff that a detailed work plan be developed as a straw man for stakeholder review so that the EMP driven activities can be properly integrated into the NERC Strategic and Operational Program Plans (e.g. RISC priority determination, Initiatives, Standards, Research, etc.). Only then can NERC resource allocation be assessed and choices made regarding what the sequence of the activity and the level of effort within the NERC fiscal reality.

Additionally, Sector 9 recognizes that there are many other agencies and industry groups that need to be involved. As the EMP Task Force has noted, some of these entities will need to take the lead with NERC in a supporting or information creation/delivery role.

NERC as a first priority should ascertain whether or not these agencies actually can and will support their proposed roles in NERC's proposed plan. Those other entities may have other competing priorities for example in other higher risk sectors (gas, water, transportation) which may pre-empt the priorities the NERC EMP TF proposes in its assessment.

A report to the NERC stakeholders regarding the feedback from these entities (DOE, DHS, NATF, FERC, etc.) regarding their acceptance of their proposed role should be prepared and delivered to the NERC stakeholders. This project should identify the timing and relative priority these other entities place on the electric delivery related EMP risk mitigation activities.

The EMP Task Force should be maintained to carry out the activities including the outreach to the other lead entities as a first priority. But NERC is a long way away from a workable plan to implement even its portion of the proposed activities. NERC's first priority should be to socialize the EMP Task Force Report with the non-NERC entities proposed to lead various efforts and obtain a time frame for their portion of the activities.

II. Supply Chain risk Assessment

The NERC BoT requests MRC policy input on the following questions regarding the Supply Chain Risk Assessment (Attachment B):

A. The NERC BoT asks whether Sector 9 agrees with the Supply Chain Risk Assessment recommendation.

Sector 9 agrees that the combined effect of a coordinated cyberattack on multiple locations could affect BES reliability beyond the local area. Also sector 9 agrees that the analysis of third-party electronic access to generation resource locations is even more concerning. Sector 9 believes that Low Impact BES Cyber Assets should be included as contemplated by FERC. Nevertheless, some Sector 9 members believe that any efforts should be appropriate to the entity's individual risks identified by a risk assessment.

B. The NERC BoT asks whether Sector 9 has an alternate way to address the identified risk in a more cost effective manner?

Much like how risk assessments are identified and used within NERC Reliability Standard CIP-003, a requirement for Supply Chain could be factored in as a part of that work. Any resulting efforts would come as a result of appropriate risk and cost-benefit analysis acceptable to the organization. This mimics the work already being recognized in the CIP-003 efforts.

MEMORANDUM

TO: Roy Thilly, Chair
NERC Board of Trustees

FROM: Carol Chinn
William J. Gallagher
Roy Jones
John Twitty

DATE: January 22, 2020

SUBJECT: Response to Request for Policy Input to NERC Board of Trustees

---

The Sector 2 and 5 members of the NERC Member Representatives Committee (MRC), representing State/Municipal and Transmission Dependent Utilities (SM-TDUs), appreciate the opportunity to respond to your January 2, 2020 letter to Mr. Greg Ford, Chair of the MRC that invited MRC member sectors to provide input on the Electromagnetic Pulse Task Force (EMP Task Force) Report (Report) and the NERC Supply Chain Risk Assessment (Assessment). We look forward to discussing the Report and Assessment along with the balance of the agenda package scheduled for distribution before the upcoming meetings of the Board of Trustees (Board), Board committees, and the MRC, on February 5-6, 2020 in Manhattan Beach, California.

Summary of Comments

- **Collaborative Electric Reliability Organization (ERO) Model**

  Stakeholders, including the SM-TDUs, believe their input developed through committees and task forces should not be mis-characterized, or modified by NERC without reasoned explanation when presented for reliability and security decisions.

- **EMP Priorities**

  The SM-TDUs support the priorities for the strategic recommendations as they were presented in the EMPTF Report. The highest priority should be assigned to the strategic recommendations related to Research and Development (R&D), followed by, or in parallel with, the strategic recommendations for Vulnerability Assessments (VA). Regardless of the priorities assigned to the strategic recommendations, it is the opinion of the SM-TDUs, that action should be taken on all the strategic recommendations.

- **Supply Chain Risk Assessment**

  The SM-TDUs do not support modifying the supply chain standards to include low impact Bulk Electric System (BES) Cyber Systems with remote electronic access connectivity. The continual revisions of the not-yet-implemented supply chain standards for high- and medium-impact BES Cyber Systems, add, rather than lessen, risk. The NERC staff assessment appropriately identifies a remote access supply chain risk but provides an

unsupported revision to the supply chain standards as the solution. The unsupported conclusion could have the unintended consequence of undermining the objectives of CIP-002. CIP-003 should be considered as the best framework for dealing with remote access risk. Creating a baseline from an implemented and audited supply chain standard for high- and medium impact BES Cyber Systems will be more valuable to the goal of diminishing supply chain risk than continually modifying the standards. Furthermore, any effort to modify the Supply Chain standards to incorporate low-impact BES Cyber Systems ought not to be considered until at least one (1) year after the July 2020 implementation date for high- and medium-impact BES Cyber Systems.

Collaborative ERO Model

The SM-TDUs have a general concern that stakeholder input developed through committees, task forces, and other working groups, should not be mis-characterized or modified by NERC in final reports or decisions unless NERC has provided a reasoned explanation to the stakeholders. This communication is important to maintain a collaborative relationship and a level of trust among the ERO.

We believe an open dialogue between the stakeholder groups and NERC is important for the continued success of the ERO. Significant stakeholder time and resources are used to provide input on reliability and security matters. While stakeholders understand that NERC does not need to accept all stakeholder input without change, there is the expectation that if NERC wishes to change conclusions or recommendations in a stakeholder-driven report/assessment, that NERC will engage with the stakeholders to provide an explanation of how the input was considered and why NERC decided to characterize the input differently, or modify the input. Often, as evidenced by the EMP and Supply Chain matters addressed in this Policy Input letter, NERC has made a decision to deviate from the stakeholder recommendations on certain matters without notice or discussion with those stakeholders. The SM-TDUs recommend that if NERC has a different opinion from a stakeholder working group report/assessment that NERC should explain its different opinion in presentations, whitepapers, etc. This is especially true for Board policy input requests that typically relate to final ERO decisions.

EMP Strategic Recommendations

Priorities

The SM-TDUs appreciated the Board's acceptance of the Report in November 2019 that included five focus areas and a list of strategic recommendations. The Board's request for input to help establish priorities for implementing the strategic recommendations is indeed timely and should support the most efficient next steps actions. The SM-TDUs agree with all the EMPTF's strategic recommendations. Also, the SM-TDUs support the initial prioritization of the strategic recommendations by the NERC staff, as indicated by those in bold letters. Furthermore, the SM-TDUs sectors believe the focus areas that should be assigned the highest priorities are first R&D, followed by or in parallel with VA. In addition, to supporting the priorities, the SM-TDUs suggest that the highest priority strategic recommendations, ought to be:

- Monitor and communicate to the industry research pertaining to EMP and EMP-related national security initiatives that impacts the BES. (R&D No. 3) (higher that R&D No. 1)

- The ERO Enterprise should develop tools and methods for system planners and equipment owners to use in assessing EMP impacts on the BPS. (VA No. 1)
- The EMP Task Force should provide guidance to industry on how to identify and prioritize hardening of assets that are needed to maintain and restore critical BPS operations. (VA No.2)

Please note that the following VA recommendation in the Report was omitted from the Policy Input letter. We view this recommendation as a high priority and consider its omission from the Policy Input letter to be a substantive oversight.

- Consider maintaining an EMP Task Force within the ERO Enterprise Technical Committees to regularly coordinate and collaborate with governmental authorities to procure and effectively disseminate information needed by industry.

Regarding this latter recommendation, the SM-TDUs believe that R&D is a critical priority due to the linkage between national defense and critical assets that could be affected by EMPs. Government agencies and their research arms have the expertise, resources, and information that the electric industry needs. Moreover, EMP research undertaken by government partners can help improve common understanding and assess the risks and gaps in knowledge. In turn, the other VA recommendations in the Report are important for ensuring that appropriate system planning decisions be made.

As was discussed at the November 2019 Board meeting, many entities will play a role in the next steps required to strategically address EMP risk. Determining a realistic order of priority can start with MRC policy input but should also include, and possibly be led by, other key stakeholders such as the Department of Defense, the Department of Energy, the Department of Homeland Security, and the Institute of Electrical and Electronic Engineers, among others. Obtaining input from the key affected stakeholders will ensure that those recommendations that are most important are addressed.

Implementation of Recommendations

The NERC Staff proposed priorities for the strategic recommendations (bold letters) in the Policy Input letter but did not provide reasoning for its proposed priorities. Furthermore, of the 13 priority items listed, 10 items have different responsible parties listed from those identified in the Report. While these differences might be explained by NERC Staff's recommendation that the EMPTF be retained as an RSTC sub-committee, there is no explanation for the recommended assignments of responsibility. The SM-TDUs believe that collaboration in the implementation of the strategic recommendations will be essential to ensure results that can be widely supported. Furthermore, involving the appropriate parties will be important to attain agreement on the priorities.

The SM-TDUs want to be clear that it should not be NERC's intent to work on a few select strategic recommendations and ignore the other strategic recommendations in the Report. The SM-TDUs sectors are not trying to suggest that "everything is a priority," but rather believe that the Report provided a package of needed actions that can be undertaken in parallel, with emphasis on

those having the highest priority. To that end, the SM-TDUs believe that a well-thought out work plan is needed to ensure that none of the issues addressed by the recommendations are neglected.

Input Letter Recommendations vs. Task Force Report Recommendations and Responsibilities

Consistent with Collaborative ERO Model item above, the recommendations as written in the Policy Input Letter are not written as they were in the Report. Some of this inconsistency is addressed regarding the assignments of responsibility for implementing the recommendation. However, there are also other wording changes that are unexplained. Therefore, SM-TDUs believe there should be adequate explanation for any inconsistencies between the wording of the Policy Input Letter and the accepted Report.

Supply Chain Risk Assessment

The SM-TDUs, first and foremost, want supply chain security risk to be addressed, whether in requirements that make sense for standards, or in other actions that address supply chain risks. While the SM-TDUs believe the Supply Chain standards begin to address associated security risks, they also believe constant revisions to standards not yet implemented, add, rather than reduce, supply chain risk. Pertinent to the Board's request about the Assessment, the SM-TDUs believe the Assessment appropriately identifies a remote access supply chain risk but provides an unsupported revision to the supply chain standards as the solution. Consequently, SM-TDUs do not agree with the NERC Staff recommendation that the Supply Chain standards should be revised to include low impact BES Cyber Systems with remote electronic access connectivity.

Consideration of NERC CIPC's Supply Chain Working Group Input

As an initial matter, the NERC Critical Infrastructure Protection Committee's (CIPC) Supply Chain Working Group (SCWG) provided technical recommendations that did not become part of the Assessment. Importantly, the SCWG raised points that, at a minimum, should have received reasoned consideration in the Assessment. Given the significant time and effort that the SCWG has provided to NERC's supply chain efforts broadly and the Section 1600 Survey specifically, SM-TDU's are concerned about the lack of consideration that the SCWG's technical input received in the Assessment.

A key point the SCWG made and that was not considered by NERC, was that "remote access connectivity" is not a defined or understood term and, therefore, a risk that is not yet specifically defined or understood. Is the risk related to third-party remote access or any remote access? The SCWG recommended that the risk to reliability is the third-party remote access, and not the overly broad statement of *remote electronic access connectivity*. The SCWG attempted to provide that focus in section d of the Section 1600 survey by limiting the applicability to row d – where the applicability was, 3.1 (Control Center), 3.2 (Transmission), 3.3 (Generation). The focused scope of the Section 1600 questions was lost when interpreted by NERC staff in the Assessment. The answer to that question is used by the Assessment to include low impact BES cyber assets in CIP-013. While the survey question was directed to a limited scope, the Assessment widens the scope without explanation.

The SCWG noted that, currently, industry is engaged in implementing the approved Supply Chain Risk Management changes (new NERC Reliability Standard CIP-013-1 and updated NERC

Reliability Standards CIP-005-6 and CIP-010-3). Furthermore, the SCWG asserted that the current CIP-013-1 standard is being modified to include Electronic Access Control and Monitoring Systems (EACMS), prior to the CIP-013-1 standard becoming effective. Accordingly, while the industry is addressing the already changing scope of the standard, discussions of further Supply Chain Standards modifications, prior to the original standard being implemented, is an overly aggressive and unreasonable approach. The original NERC Reliability Standard should be implemented and audited through at least one audit cycle to allow for an appropriate baseline.

The Assessment - CIP-002 and CIP-003

The SM-TDUs believe the Assessment could have the unintended consequence of undermining the objective of CIP-002. The current CIP standards have appropriately considered each individual asset as having a low impact to the BES. Therefore, the CIP-002 model treats sites at the asset level and protecting the site as one "asset containing lows," rather than at an individual cyber asset level due to their low impact and significant number. If the Assessment recommendation means adding low impact BES Cyber Systems to the supply chain standards (CIP-013 and certain CIP-005 and CIP-010 requirements), it conflicts with the CIP-002 model and would first require an extensive CIP-002 rewrite. Those supply chain standards were not designed for the "asset containing lows" model but do fit with the high/medium impact cyber asset/system level model.

If the conclusion is that remote access risk needs to be addressed, then SM-TDUs believe the appropriate place to consider that risk is in CIP-003 under Section 3 of Attachment 1. The CIP-003 standard will be consistent with addressing low impact BES Cyber Systems and will allow for a standard revision that can be written in a way that is only applicable to those devices that meet the requirements of Section 3.1 of Attachment 1 with an addition for remote access. Importantly, it will provide the appropriate framework for establishing a standard authorization request (SAR).

Timing of Section 1600 Survey and Supply Chain Security and Risk

NERC issued the data request in late summer 2019, which occurred while entities subject to the medium/high impact requirements of CIP-013 (and certain CIP-005 and CIP-010 requirements) were amid developing strategies and implementation plans for the requirements. Over the past 6-9 months, registered entities, through small group sessions and other efforts, have been working with NERC and industry peers to understand practices that might be applied to ensure compliance with the requirements.[1] Only within the last few months have many registered entities begun to coalesce around the best approaches to manage supply chain risk. In turn, there are several ongoing initiatives in the industry to develop protocols, practices, etc.

One such initiative is being led by the North American Transmission Forum (NATF) to develop supply chain cyber risk criteria for supplier evaluation that can be mapped to risk assessment questions. A primary challenge faced by the NATF has been dealing with the scope of complying with the supply chain standards versus the scope of ensuring security. A complicating factor is that registered entities can only request that suppliers and vendors cooperate and cannot direct their compliance with security-based questionnaires. The effort seeks to ensure that the questions can address the compliance requirements and increase coordination and cooperation with suppliers and vendors; a key challenge.

[1] Cite Large Public Power Council workshops, American Public Power Association workshop, NATF meetings

The NERC staff proposal for adding low impact BES Cyber Systems to the supply chain standards implicitly adds burden to the already challenged utility and supplier/vendor relationship before the currently approved standards' initial effective date. It will change the scope of the standards and will cause changes to both the criteria and questions that industry and suppliers/vendors have been challenged with, to date. This constant change, which does not allow a baseline to form, only increases overall supply chain risk for utilities.

The Assessment contends that, based on the data feedback, a broad coordinated attack on low impact facilities would be a risk to the BES. The assessment reaches this conclusion with little, to no support. In the SM-TDU April 2019 policy input, we questioned NERC's use of the 1600 form to gather information when the questions would relate to actions required by a standard not yet in place. In other words, the survey would be premature, if questions were framed as if compliance measures were already in place. In sum, we do not agree with the risk that NERC has identified, especially when based on premature and incomplete data. NERC should develop a more rigorous process to determine the real risk. This process should be scheduled for a time at least a year following implementation of the current medium/high impact facilities standards. A year's worth of information will be valuable for NERC to make an informed decision.

We encourage more time for NERC to conduct a comprehensive risk assessment using actual input and data from the industry based on experience and information after implementing the current standards that apply to medium/high impact facilities. NERC should start a low-impact assessment after July 2021 (a year after the effective date of the current standards) so actual experience can be used as a roadmap for the assessment. Depending on how entities implement the current standards, and how NERC and the Regional Entities audit compliance with the standard, this could change the risk assessment as it applies to low-impact facilities. We propose that NERC consider asking entities to share best practices regarding management of remote access in an informal session to allow compliance monitoring teams to gather information without attribution to a specific Registered Entity. This may be facilitated by adding an additional item to the CIP-003-7 RSAW Electronic Access Controls Implementation Study concerning what controls a Registered Entity has put in place that mitigate the risk of remote access. This information could help better inform NERC of what, if any, risks there are to a "coordinated cyber-attack". If there is concern over the use of compliance engagements, we recommend that the members of the MRC gather similar information for guidance in developing the next steps.

Assuming there is a risk to the BES, an alternative way to address this in a more cost-effective manner is to use the NATF industry collaboration initiative to develop guidance and tools for the industry to identify opportunities to manage risk.

Thank you for the opportunity to provide this policy input. We look forward to the discussion at the meetings.