# 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.

###