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.

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.