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: July 26, 2017

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 July 5, 2017 letter requesting policy input in advance of the August 9-10, 2017 NERC Board of Trustees meetings.

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

CELEBRATING 30 YEARS
LPPC
LARGE PUBLIC POWER COUNCIL

MEMORANDUM

TO: Roy Thilly, Chair
NERC Board of Trustees

FROM: Carol Chinn
Vicken Kasarjian
William J. Gallagher
David Osburn

DATE: July 26, 2017

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 letter dated July 5, 2017 to Mr. John Twitty, Chair of the MRC, requesting policy input on Supply Chain Risk Management during the upcoming meetings of the NERC Board of Trustees (BOT), Board committees, and the NERC MRC on August 9-10, 2017. The letter also notes three other topics and associated documents for ongoing stakeholder comments.

Summary of Comments

- **Item 1: Supply Chain Risk Management**
  - SM-TDUs recommend that prior to implementation of the Supply Chain standard, NERC integrate the standard into its work on consistency, replicate pre-implementation CIP Version 5 efforts, and communicate with stakeholders prior to implementation how endorsed implementation guidance will work.
  - To best evaluate the effectiveness of the Supply Chain standards the SM-TDUs believe that NERC should establish a baseline for vendor security before the effective date of the standard that can be measured against during implementation.
  - While SM-TDUs believe that excluding low-impact BES Cyber Systems from CIP-013-1 appropriately addresses the Commission's directives and that much of the risk is mitigated, we believe that NERC should continue to evaluate the risk created by supply-chain issues for low-impact BES Cyber Systems.
  - More can, and should be done to address the cyber risks to electric utilities, but these efforts should be focused on voluntary programs being developed beyond the NERC standard development process.
- **Other Policy Input Items**

- SM-TDUs will provide specific input on the distributed documents at the BOT and MRC meetings.

- NERC should include stakeholders in the standard review project (Paragraph 81) from the outset to gain a vantage that only stakeholders can provide.

- Public power looks forward to the discussion on the most important priorities the ERO should pursue over the next 5-7 years.

Item 1: Supply Chain Risk Management

The BOT seeks input from MRC sectors on four specific questions regarding the developing Supply Chain Risk Management standard. The following is the SM-TDU's responses to those questions:

1. *What activities or studies NERC should engage in between now and the effective date of the new and modified standards to support effective implementation?*

Because the Supply Chain standard is new and complex, similar to the versions of the Critical Infrastructure Protection (CIP) standards, SM-TDUs recognize that implementation will be challenging. SM-TDUs believe there are several areas that NERC and industry have been working on that should continue to be honed with an emphasis on timing and substance prior to the Supply Chain standard's implementation date. Prior to implementation, SM-TDUs recommend that NERC continue its work on consistency (integrating the Supply Chain standard), replicate the CIP Version 5 efforts, and stress how endorsed implementation guidance will apply upon implementation of the standard.

Compared to traditional standards, the CIP standards are more challenging and more complex for registered entities to implement. Different Regions with a multitude of auditors multiply the challenge of implementing new CIP standards. Due to their experience with previous CIP standard implementation, SM-TDUs' registered entities are concerned that the various Regional Entities will interpret the new standard and guidance differently. Consequently, regional consistency is an issue that needs to be addressed prior to implementation of the Supply Chain standard. Currently, the NERC Board and Compliance and Certification Committee (CCC) have been working on consistency which is an effort SM-TDUs support. The SM-TDUs encourage NERC to integrate that work with the implementation of the Supply Chain standard to ensure that the past experience with CIP standards is not repeated with the Supply Chain standard implementation.

SM-TDUs recommend replicating the pre-implementation CIP Version 5 efforts with Supply Chain standard prior to its implementation. The rollout of CIP Version 5 included collaborative development with industry of FAQs, white papers, and pilot programs prior to implementation. SM-TDUs found those materials and processes facilitated a more efficient and effective rollout of CIP Version 5 than otherwise would have been the case. In addition, as part of pre-implementation activities, SM-TDUs appreciate the Supply Chain standard drafting team producing, and NERC endorsing, the implementation guidance which provides complying entities with greater clarity, prior to the implementation of the standard.

The Compliance Monitoring and Enforcement Program (CMEP) Practice Guide makes clear that if the Implementation Guidance is followed by a registered entity, NERC compliance and enforcement staff will consider such guidance as a possible method to achieve compliance. We understand that, if a registered entity follows the endorsed Implementation Guidance, NERC compliance and enforcement staff will give deference to the Implementation Guidance. And Regional Entities would be bound as well to give the same deference. There may be other ways to comply outside of the guidance, but at that point the registered entity would not have the protection of the Implementation Guidance. SM-TDUs ask NERC to highlight to registered entities and Regional Entities during the pre-implementation phase how endorsed implementation Guidance will operate upon implementation.

2. *How should NERC evaluate the effectiveness of the standards going forward?*

To best evaluate the effectiveness of the Supply Chain standards, the SM-TDUs believe that NERC should establish a baseline for vendor security (or security under the standard) before the effective date of the standard. Once the standard becomes effective, a second, comparable measure should be taken and compared to the baseline. This before-and after-analysis will show what new protections are being provided by the standard and provide valuable information on implementation status.

Evaluating the effectiveness of the Supply Chain standard needs to include an analysis of whether the standard inadvertently disrupts existing procurement practices that benefit customers. SM-TDUs want to bring to NERC's attention that public utilities have different contracting options compared to other utility ownership forms. Specifically, many public power entities rely on, or are required to use, **"**state rider" master agreements. These agreements allow public utilities to purchase as a group, with other state entities, software or hardware to achieve economies of scale. The state or city negotiates purchases that public power utilities, and in turn their customers, benefit from. Public power utilities have a concern that the standard may directly or indirectly limit the use of these contracts. Either the standard's requirements could directly limit the use of this type of contract, or the standard could create a level of uncertainty which causes entities to shy away from using such contracts if permitted by law. A parallel example is how CIP-004 R4-5 and CIP-011 R1 together have chilled use of cloud-based storage.

Accordingly, as part of its evaluation NERC needs to ensure that the Supply Chain standard does not cause registered entities to avoid using state-rider master agreements for fear of auditors not accepting the contracts. Requiring a separate purchase by a utility would unnecessarily increase costs and cause delays in procurement, both of which could end up actually having detrimental effects on the overall security of the system.

3. *What risks and related issues should NERC continue to study on a collaborative basis related to the challenges of cyber security supply chain risk management, including risks related to low impact BES Cyber Systems not covered by the standards?*

The removal of low-impact BES Cyber Systems from CIP-013-1 appropriately addresses the Commission's concerns as specified in Order No. 829 and fulfills the Order's request for a risk-based approach. Application of Standard CIP-002 is an established, Commission-approved approach to categorize a utility's BES Cyber Systems into high, medium, and low risk

classifications. Application of this established risk-based approach to cyber asset procurement for electric utilities is natural, appropriate, and consistent with the guiding CIP philosophy, stated in Section 6 of each CIP Standard, that each Standard "exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems."

SM-TDUs also believe that the risks of excluding low-impact BES Cyber Systems from CIP-013-1 are mitigated by the fact that many entities with low-impact systems also have medium- or high-impact BES Cyber Systems. Such entities can and should, as a matter of normal business practice, adopt the same supply chain practices for their low-impact systems as they are required to implement for their medium- and high-impact systems.

While SM-TDUs believe that excluding low-impact BES Cyber Systems from CIP-013-1 appropriately addresses the Commission's directives and that much of the risk is mitigated, we believe that NERC should continue to evaluate the risk created by supply-chain issues for low-impact BES Cyber Systems. To the extent that NERC identifies risks that warrant mitigation, NERC should determine whether those risks can be best addressed through more flexible non-Standard approaches that are better adapted to addressing rapidly evolving cyber threats.

4. *For assets that are not subject to the new cyber security supply chain risk management requirements, are there other actions NERC should take to address potential supply chain risks, such as developing guidelines, presenting webinars and/or collaborating with the Forums and small system representatives on strategies and best practices?*

As NERC has noted in the past, not every protection of the Bulk Power System (BPS) is best accomplished through a standard. The SM-TDUs appreciate NERC communicating and justifying such realities to FERC that not all security issues can be resolved through reliability standards since there are other safeguards. Public power stated at the recent FERC Reliability Technical Conference that more can and should be done to address the cyber risks to electric utilities, but that alternative approaches to standards could be more effective, more flexible, and less costly. The last thing we want to do is adopt standards that dictate expensive and obsolete solutions to threats that have morphed.

Alternative approaches to address supply chain risks could include workshops held by NERC and Regional Entities to educate industry about effective strategies for enhancing the reliability and security of supply chains, and the development and publication of best practices. Webinars, as well as collaboration with Forums and small system representatives, are also effective ways of disseminating best practices and lessons learned.

In addition, voluntary programs being developed beyond the NERC standard development process can effectively address cyber risks. An example of such a program is APPA's cooperative agreement with the U.S. Department of Energy (DOE). Under this agreement, APPA is undertaking an extensive multi-year, multi-task project of improving the cyber resiliency and security posture of public power utilities. The project goal is to improve the resiliency and cybersecurity infrastructure within public power utilities and one of the modules specifically

addresses supply chain. As the effort moves forward, public power would be happy to speak with NERC about the program.

Lastly, we see value in engaging with governmental entities such as the Department of Homeland Security and the Department of Energy on an overarching strategy regarding supply chain cyber security that goes beyond our mandatory standard sector. Supply chain security poses an economy-wide challenge that is not limited to the electric sector, and an overarching strategy can be done in a manner that fully engages responsible suppliers with whom public power utilities and other sectors do business. Similar to DOE's Electric Sector Cybersecurity Capability Maturity Model (C2M2), a unified effort could lead to a set of common practices or protocols to which entities in electric supply chain may subscribe, and upon which the electric sector may rely.

Other Items and Documents

The SM-TDUs request that more time be provided to sufficiently review the documents that are noted in the policy input letter (2018 Business Plan and Budget: ERO Enterprise Long-Term Strategy, Operating Plan, and 2018 Metrics; Special Reliability Assessment: Single Points of Disruption), and provide written input. While we understand that the documents were scheduled to be distributed in mid-July and voted on or discussed at the August BOT meeting, the documents were not part of the Policy Input Letter accordingly it is difficult for the industry to provide meaningful written input in advance of the BOT meeting. The SM-TDUs raised a similar rushed timing concern in its August 2016 policy input letter response regarding reliability assessments.

Additional Issues

The SM-TDUs appreciate and support NERC's efforts to embark on an overall review of the standards/requirements to assess their impact on reliability and recommend retirement of those that are not performance-based or otherwise do not improve reliability. Thus far, this effort has been referred to as the second Paragraph 81 project.

Public power believes that including and engaging stakeholders from the outset of this standard and requirement review project can greatly increase its success. NERC mentioned that it will begin the review process by looking at historical statistics associated with the standards and their requirements as part of scoping the project. Stakeholder input can add insight to such a look-back. Stakeholder's real world experience complying with the standards can add qualitative information on standard requirements that can be provided by no other party. Such insight will add to the historical statistics and assist NERC in performing a comprehensive scoping for the review of the standards/requirements in a second Paragraph 81 project.

As the SM-TDUs understand from the July 13, Trades and Forums meeting at NERC, the second Paragraph 81 project work has begun, with NERC looking at scoping the project. Public power entities are in the process of reviewing documents that would be impacted by the second Paragraph 81 projects, such as the draft Reliability Standards Development Plan (RSDP) (comments due July 25), NERC 2018 Business Plan and Budget (comments due July 27) and ERO Enterprise Long-Term Strategy, Operating Plan and 2018 Metrics ERO (comments due August 17). We expect that these documents will ultimately include specific Paragraph 81 plans and goals for NERC in 2018.

SM-TDUs believe that NERC should work with stakeholders, possibly through Trade representatives, to quickly determine the best way of scoping the second Paragraph 81 effort and then incorporate into the NERC plans and goals.

SM-TDUs appreciate BOT Chair Thilly's request in the policy input letter for MRC members to be prepared to provide and discuss the three most important goals for the ERO to achieve over the next 5-7 years. The public power MRC representatives stand ready and look forward to the discussion.

Thank you for the opportunity to provide this policy input.