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: April 24, 2019

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 April 2, 2019 letter requesting policy input in advance of the May 2019 NERC Board of Trustees meetings.

MEMORANDUM

TO: Roy Thilly, Chair
NERC Board of Trustees

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

DATE: April 23, 2019

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 April 2, 2019 letter to Mr. Greg Ford, Chair of the MRC that invited MRC member sectors to provide input on the NERC Draft Cyber Security Supply Chain Risks – Staff Report and Recommended Actions (Draft Report). We look forward to discussing the Draft Report, along with the balance of the agenda package scheduled for distribution before the upcoming meetings of the Board of Trustees (BOT), Board committees, and the MRC, on May 8-9, 2019 in St. Louis, Missouri.

Summary of Comments

- **Draft Cyber Security Supply Chain Risks Report**
  - **Assessing the Risk of Low-Impact BES Cyber Systems.**
    - NERC should not use its compliance/enforcement authority to collect information about registered entities' implementation of voluntary practices.
    - Given the importance of collecting the right information, the report should not prejudge the content of the Section 1600 data request.
    - NERC should reconsider the scope, charter, and membership of the CIPC Supply Chain Working Group in light of the significant role envisioned for that working group.
    - Any new Security Guidelines should follow the CIPC's established approval process for such guidelines.
    - The Security Guideline for low-impact BES Cyber Systems could fully or partially adopt the APPA/NRECA Whitepaper.
  - **Supplier Accreditation Process**
    - The ERO should encourage the development of an appropriate supplier accreditation process that supplement and/or support the objectives of the NERC Supply Chain standards.

SM-TDUs Policy Input on the Draft Cyber Security Supply Chain Risks Report

The SM-TDUs appreciate the Board's continued commitment to seek policy input from the MRC in advance of the quarterly Board and MRC meetings. The following are the views of the SM-TDUs regarding the issues and associated questions raised in the Board's letter to the MRC regarding the Draft Report.

A. General Comments on the Draft Report

First, the SM-TDUs would like to thank the NERC Board of Trustees for taking the approach they did in undertaking the preparation of the Draft Report that started with the August 2017 BOT resolutions. The Resolutions called for APPA, working with LPPC and TAPS, and in conjunction with NRECA, to provide the white paper: Managing Supply Chain Risk – Best Practices for Small Entities. We appreciate the extent to which the White Paper informed the Draft Report, and believe it serves as a valuable resource for public power and cooperative utilities.

The SM-TDUs generally support the Draft Report and recognize it as an important step forward for grid security. Evolving cyber security risks place a premium on agile processes for risk identification and mitigation. By the same token, mitigating supply chain risk will require continuing actions to maintain and improve security. The Draft Report provides a good baseline on which to build on further analysis and action to secure the grid from the supply chain risk. Consistent with the risks identified in the Draft Report and the directives contained in FERC Order No. 850, the Draft Report recommends revising the Supply Chain Standards to include Electronic Access Control and Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) that provide electronic access to high and medium impact BES Cyber Systems. SM-TDUs agree that these are appropriate steps. The SM-TDUs also support the Draft Report recommendation that the Supply Chain Standards not include low-impact BES Cyber Systems at this time.

The Draft Report also includes recommendations for next steps associated with low-impact BES Cyber Systems, and a supplier accreditation process or processes. It is on these next steps the SM-TDUs herein provide comments.

B. Comments on the Draft Report Recommendations for Low-Impact BES Cyber Systems

1. NERC should not use its compliance/enforcement authority to collect information about registered entities' implementation of voluntary practices.

The Draft Report (at Page 20) indicates that NERC will use pre-audit surveys and questionnaires to collect information about "actual market and entity practices following implementation of the Supply Chain Standards and the extent to which these practices may help reduce risks to reliability stemming from the supply chains for low impact BES Cyber Systems." The Draft Report (at Page 24) characterizes these pre-audit surveys and questionnaires as "voluntary efforts to obtain risk data."

In other words, an ERO auditor will ask a registered entity to "voluntarily" answer questions about the entity's compliance with a "voluntary" Security Guideline. In reality, given the auditor's extensive discretion and authority to enforce mandatory standards, a registered entity will not perceive the auditor's request as voluntary.

NERC and its Regional Entities lack authority to enforce voluntary security practices that have not gone through the established standard development process and been approved by FERC. If Registered Entities perceive that NERC is using its audit process to indirectly achieve the same result, it would call into question the integrity of NERC's compliance/enforcement processes. NERC should, therefore, avoid entangling its compliance/enforcement activities with its information gathering activities.

Of course, an auditor can properly ask about how an entity categorized its BES Cyber System as low or medium impact, to assess compliance with CIP-002. And an auditor could ask broader questions about supply chain management practices, including supply chain practices for low impact BES Cyber Systems, as part of an effort to scope an audit of the entity's compliance with CIP-013 for its medium and high impact BES Cyber Systems.

But if a registered entity has correctly concluded that it has no medium or high impact BES Cyber Systems and is thus not subject to CIP-013, there is no compliance/enforcement purpose behind asking about that entity's voluntary supply chain practices for its low impact BES Cyber Systems.

NERC has many tools for information gathering, including NERC Alerts and Section 1600 data requests. To that end, the trade associations, such as APPA, LPPC and TAPS can help NERC obtain robust response rates from registered entities to voluntary questionnaires. NERC certainly needs good information about voluntary practices that registered entities are implementing to secure the BES and improve reliability. But NERC must maintain a clear distinction between those information gathering activities and its compliance/enforcement activities.

2. *Given the importance of collecting the right information, the final report should not prejudge the content of the Section 1600 data request.*

The Draft Report (at Page 20) states that "at minimum" a Section 1600 data request would include questions to determine the incremental costs to extend CIP-013 to low impact BES Cyber Systems with External Routable Connectivity and questions about the number of low impact BES Cyber Systems with External Routable Connectivity. Collecting data on the scope of BES Cyber Systems and the costs of supply chain practices is very important and would benefit from thorough stakeholder input so that the questions asked result in meaningful responses that can guide decision making.

We support the use of a Section 1600 data request to collect information about the number of BES Cyber System at each impact level. Other aspects of the proposed Section 1600 data request might need to be delayed or further refined for the information collected to be useful. With respect to costs, the Draft Report's proposed questions may be premature. And with respect to External Routable Connectivity, the Draft Report's proposed questions are overly prescriptive. The Board

should ensure that the Section 1600 data request follows the established process, and that nothing in the final report is intended to (or will) prejudge what questions ultimately get asked.

(a) It is premature to estimate costs associated with extending CIP-013 to low impact BES Cyber Systems.

Asking questions now about the incremental cost of extending CIP-013 to low impact BES Cyber Systems is unlikely to produce meaningful results. A significant impact of CIP-013 will be the increased cost of procuring goods and services; but until registered entities start requiring their vendors to implement certain supply chain risk management practices, no one will know how much vendors will increase their prices. It may be more prudent to delay asking questions about costs but doing so will be difficult if the Board approves the Draft Report that seems to prejudge the minimum requirements for the Section 1600 data request.

(b) NERC should not prejudge whether External Routable Connectivity is the sole factor for determining the enhanced risk of low impact BES Cyber Systems.

The Draft Report suggests that low-impact BES Cyber Systems with External Routable Connectivity are higher risk than low-impact systems without External Routable Connectivity. External Routable Connectivity may be too blunt a concept to properly distinguish risk associated with low impact BES Cyber Systems.[1] Other, more tailored, risk factors related to connectivity might include: whether remote access is permitted; whether the system allows for bidirectional or only unidirectional data flows; whether inbound/outbound communications are monitored in real-time. Also, the size of the asset associated with a low impact BES Cyber System is also a relevant risk factor (a 25 MW generator does not pose the same risk as a 1499 MW generator, but both are categorized as low impact).

Additionally, focusing on External Routable Connectivity may not address the risk associated with common mode vulnerabilities, which the Draft Report (and the EPRI report) identify as a threat related to low impact BES Cyber Systems. The Draft Report correctly concludes further study is needed to determine the potential risk of a common mode vulnerability affecting numerous low impact BES Cyber Systems.

The Draft Report recommends that, at minimum, the Section 1600 data request ask how many low impact BES Cyber Systems have External Routable Connectivity. Rather than include such a specific recommendation regarding the content of the data request, the final report should ask NERC staff to do further analysis, with stakeholder input, to better refine the attribute(s) that significantly affect the supply chain risk associated with low impact BES Cyber Systems, and which merit inclusion in a Section 1600 data request.

3. *NERC should reconsider the scope, charter, and membership of the CIPC Supply Chain Working Group in light of the significant role envisioned for that working group.*

[1] Additionally, the definition of External Routable Connectivity—"The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection"—does not necessarily fit with low impact BES Cyber Systems, which do not have Electronic Security Perimeters.

The Draft Report identifies several potential roles for the CIPC Supply Chain Working Group: assisting in the development of voluntary guidelines, determining the scope of Section 1600 data requests, and developing a plan to evaluate the effectiveness of the Supply Chain Standards. Many of those tasks are not within the scope of the CIPC Supply Chain Working Group's current charter. If the working group's charter is expanded to include these new duties, NERC should consider how the membership and voting structure of the working group should also change to ensure meaningful representation from stakeholders who will be impacted by the working group's actions. Additionally, given the working group's important role, the charter should be revised to ensure full transparency so that all stakeholders are aware of the decisions and proposals being made by the working group.

4. *Any new Security Guidelines should follow the CIPC's established approval process for such guidelines.*

The CIPC Charter, approved by the Board in February 2018, includes an appendix describing the process the CIPC must follow to develop a new or updated Security Guideline.[2] The CIPC Charter (at Page 5) recognizes that Security Guidelines "are not binding norms or mandatory requirements" but they "may be adopted by a responsible entity in accordance with its own facts and circumstances." It also recognizes that because Security Guidelines "contain suggestions that may result in actions by responsible entities, those suggestions must be thoroughly vetted before a new or updated guideline receives approval by a technical committee." Therefore, it establishes a transparent process for approving Security Guidelines that includes solicitation and consideration of stakeholder comments.

The CIPC Supply Chain Working Group's existing charter does not give that working group independent authority to develop Security Guidelines, although the CIPC Charter does allow for the CIPC to delegate certain tasks to a committee subgroup. If the CIPC Supply Chain Working Group receives such delegated authority, any Security Guidelines must follow the CIPC Charter's established approval process. If the CIPC Supply Chain Working Group's charter is revised to allow it to develop its own Security Guidelines, then the revised charter should adopt an approval process substantially similar to the CIPC's.

Importantly, the CIPC approval process ensures that the committee itself—not NERC staff—is ultimately responsible for the Security Guideline. In contrast, the Draft Report suggests that NERC staff should develop the Security Guideline, in consultation with the CIPC Supply Chain Working Group. That would subvert the established, Board-approved process for developing Security Guidelines.

NERC staff must, of course, play an important role in developing the Security Guidelines. Given the importance of supply chain issues, NERC should dedicate adequate staff to support the development of the Security Guidelines. However, the ultimate responsibility and authority for developing/approving the Security Guideline must remain with the CIPC or CIPC Supply Chain Working Group.

---

[2] https://www.nerc.com/comm/CIPC/Related%20Files%20DL/CIPC%20Charter%20%20Board%20Approved%202018.pdf

5. *The Security Guideline for low impact BES Cyber Systems could fully or partially adopt the APPA/NRECA Whitepaper.*

The Draft Report states (at Page 23) that "NERC staff expects entities that own only low-impact BES Cyber Systems to develop supply chain risk management programs tailored to their unique risk profiles and priorities." Further the Draft Report states (at Page 23) that NERC staff, in consultation with the CIPC Supply Chain Working Group, will develop a "security guideline" to assist entities in "voluntarily applying supply chain risk management plans to low-impact BES Cyber Systems."

The NERC Board already requested that APPA and NRECA develop a whitepaper identifying effective supply chain risk management practices for small entities. That whitepaper has been cited extensively in the EPRI report and the current Draft Report. Moreover, the Draft Report properly identifies the whitepaper as a resource for entities that own only low-impact BES Cyber Systems in developing voluntary supply chain risk management programs. Therefore, it may not be necessary to expend significant resources developing a new Security Guideline.

When developing the new Security Guidelines, the CIPC Supply Chain Working Group (supported by NERC staff) may conclude that the APPA/NRECA Whitepaper is a sufficient foundation on which entities with only low-impact BES Cyber Systems can build their own tailored voluntary supply chain risk management program for those systems. In that case, the Security Guideline for low-impact BES Cyber Systems could simply refer to the APPA/NRECA Whitepaper. The report should be revised to acknowledge that, by calling for a new Security Guideline, NERC is not predetermining that anything more than the APPA/NRECA Whitepaper is necessarily required.

C. Comments on the Draft Report's Supplier Accreditation Process

SM-TDUs strongly support the development of a supplier accreditation process (or processes) as a supply chain security practice. SM-TDUs welcome NERC's endorsement of a supplier accreditation process as a best aspirational practice but believes there is much organizational work to be done before this approach can be widely adopted. In turn, the SM-TDUs encourage NERC to step up to facilitate the development of accreditation processes. To this end, SM-TDUs believe that NERC, as the FERC approved ERO and as a leader in electric reliability and security, can use its standing to encourage the development of an appropriate process that will supplement and/or support the objectives of the NERC Supply Chain standards. Currently, there are several efforts underway to discuss and consider options for developing a BES cyber systems supplier accreditation process that could benefit from NERC's leadership. However, it is not clear which, if any of them, are appropriate or implementable for this purpose. A more holistic approach is required to develop a process/mechanism that suppliers, the industry, and NERC can support.

The Draft Report (at Page 3) recommends that "[e]ntities should include an independent assessment or third-party accreditation process of their vendors as part of their supply chain risk management strategy." SM-TDUs believe that this approach is premature and suggest making it an option, changing the word "should" in the quoted passage to "may." This is particularly important because significant matters regarding an accreditation process or processes remain unsettled, including the scope of assets or services subject to accreditation and the question whether

accreditation should be provided only through independent third-parties and what credentials those parties might possess.

SM-TDUs urge NERC and others to expedite work on supplier accreditation, given the pending compliance date for CIP-013. However, it is not reasonable to expect that a supplier accreditation process can be implemented 12 months from the effective date of CIP-013-1 (Draft Report, pp. 24-25). Since both NERC and industry want an effective implementation of the standard, we encourage NERC to work with stakeholders to scope a path forward on a supplier accreditation process that would include a reasonable project schedule/timeline.

At this time, the list of potential BES cyber systems vendors that may be subject to accreditation is not known. While some larger vendors appear to be receptive to the new supply chain verification process, this is largely because they already have adopted such practices for business reasons. However, smaller vendors have not had that luxury and may find that commitments to security accreditation might limit their competitiveness. When considering the accreditation process, NERC should factor in the potential that it may unreasonably limit the number of vendors available to the industry. Decision-makers should have the flexibility to balance the security benefit of the accreditation process with the economics of supply in certain supply markets.

Finally, the Draft Report uses the term "independent assessment" and "third-party accreditation," somewhat interchangeably. The difference ought to be better defined in the report. The entities available to perform independent assessments, and their associated expertise and cost, may vary depending on how these terms are defined. NERC needs to be clear regarding the terms and what NERC will and will not accept with a full consideration of how it may affect the cost for complying entities. For these reasons, public power believes NERC needs be an active participant in the development of a supplier accreditation process/mechanism.

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