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
Terry Huval, Executive Director, Transmission Access Policy Study Group

DATE: October 21, 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 September 30, 2020 letter requesting policy input in advance of the November 2020 NERC Board of Trustees meetings.

MEMORANDUM

TO: Roy Thilly, Chair
NERC Board of Trustees

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

DATE: October 21, 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 September 30, 2020 letter to Jennifer Sterling, Chair of the MRC that requested MRC member sectors to provide input on NERC's "Framework to Address Known and Emerging Reliability and Security Risks" whitepaper, as well as what should be three priorities for NERC to accomplish in the next three years. We look forward to discussing the policy input and other agenda items during the virtual meetings of the Board of Trustees (Board), Board committees, and the MRC, on November 4-5, 2020.

Summary of Comments

- **Risk Framework**
  - **SM-TDUs believe the Risk Framework steps are well formed and appreciate the effort.**
  - **The Framework needs more process and implementation detail.**
    - **Details regarding validation and addressing risk elements outside of the ERO's purview should be part of the Framework. Process transparency should be amplified.**
    - **A smaller triage group should be formed for risk validation and prioritization.**
- **NERC 3 Year Priorities**
  - **Improved Actionable Intelligence (E-ISAC strategic plan)**
  - **Standards Efficiency Review – Phase II**
  - **ERO Assisting with Engagement with Third Party Suppliers**

Risk Framework

The SM-TDUs appreciate the significant work that went into preparing the Risk Framework whitepaper that does a good job of beginning to lay out a process for addressing risks that face the security and reliability of the Bulk Electric System (BES). Further, the inclusion of the Reliability Issues Steering Committee (RISC) and RSTC in the process is appreciated. However, the process as laid out needs more detail on how the collaboration process with industry will work in practice and how priorities will be determined. Below the SM-TDU sectors offer comments on the Framework document and the Board's questions in the policy input letter. In doing so, the comments include recommendations on Framework areas where more detail on implementation of the process are offered.

Risk Framework Questions

1. Are there any ERO policies, procedures, and/or programs that are missing or need amplification?

Generally, the SM-TDUs believe that the Risk Framework paper process steps are well formed. However, what is not apparent from the process steps are specifics about how the collaborative process will work and decisions made, as the Framework steps are implemented. This is particularly true for the identification and prioritization steps.

For example, the RISC identified 10 risks in its 2019 report for either "management" or "monitoring." The Framework acknowledges collaboration with the RISC but does not offer specific details on how the 10 risks would be considered under the Framework and next steps decided. It would be helpful if the Framework paper detailed how management versus monitored risks would work within the Risk Framework process.

The Framework model appears to assume that all identified reliability and security risks will fall under the purview of the ERO and be completely mitigated by the ERO. This is simply not the case. Risks related to natural gas interdependency, electromagnetic pulse, and more recently telecommunication equipment and services, are just a few examples of issues that have several aspects that are not within the complete purview of the ERO to address or mitigate. SM-TDUs believe this is an important part of the process that needs to be detailed for the Framework to be effectively implemented.

Risk identification and validation needs to include a process that recognizes what is, and what is not, within the purview and control of NERC. Such recognition will help determine prioritization and the potential mitigations that the ERO can effectively pursue. Any ERO mitigation efforts that duplicates or works against mandates or guidelines outside of NERC's purview, would counterproductive and not be in the best interest of promoting grid reliability.

2. Does the iterative six-step risk management framework provide a sound basis for risk identification and mitigation?

As was characterized by NERC during the MRC pre-meeting webinar, the six-step risk management framework can be likened to the steps used by many risk-management processes.

Whether the basis is sound or not depends on the details associated with each step and how they are implemented. It is important for the process to be transparent. Stakeholders need to be engaged to identify on-the-ground operational risks and must be informed about risks from sources outside the industry.

All entities that engage with the ERO need to be aware of the risk process to understand what NERC is addressing and to what extent identified and validated risks present risk to the BES. The balance of the appropriate level of transparency will require the engagement of the ERO's counsel with stakeholders' counsel to determine the appropriate level of transparency for a given risk. In addition, direct engagement by the RISC is critical and appropriate RISC input should be obtained for leading risks. Further, the list of ways the ERO identifies risk on pages 4-5 of the Framework lays out a comprehensive list of ways that the ERO has established to identify risks.

As noted above, a place that SM-TDUs believe needs to be better detailed is once a risk is identified, to what degree is that risk the responsibility of the ERO before actual mitigation can be addressed. Identification, validation and prioritization all need to be considered as part of the process of determining to what extent and/or whether the risk is in the purview of the ERO. For example, is the scope of a security issue one of national security or is the security issue completely within the scope of the ERO to mitigate?

3. Are there any significant steps missing from the iterative risk management framework? If so, what steps do you propose adding?

The SM-TDUs do not believe there are steps missing but that there are process steps inclusive to the six steps, that need to be added and documented. Already mentioned are the validation/prioritization triage group, a process for distinguishing items outside of the ERO's purview and transparency considerations for each validated risk. Moreover, the MRC pre-meeting call identified the need for more detail on the formation and responsibilities for developing and maintaining the Risk Register, with which we agree.

4. Are there any missing key elements in the RSTC/RISC triage approach? If so, what key elements do you propose adding?

The SM-TDUs believe it would be useful for the process to include a specific smaller triage group that would be formed to initially evaluate, validate and prioritize risks. The group would both validate (or not) risks as they are presented and then prioritize validated risks. Validation and prioritization would be separate actions that could be done under the second step of the Framework steps. Rather than have risk consideration performed by 60 or more individuals (ERO Staff, RISC and RSTC), a smaller triage group would be more effective and efficient. Much like Standard Authorization Requests (SARs) can be offered by ERO Staff or the general public, the same would be true for risk consideration requests. SM-TDUs suggest the ERO Staff, RISC and RSTC each could select two members to serve on this validation group. The group then could add two subject matter experts (SMEs) for the particular risk under consideration. SM-TDUs believe these SMEs could come from Staff, the RISC or RSTC. Additionally, SMEs from the Standards Committee and the Compliance and Certification Committee (CCC) should be considered.

Especially when mitigation is under consideration, the CCC is a key group that should be included in the process. SM-TDUs believe it would be valuable to include the CCC with respect to mitigation decisions because this is an area that they have specific experience with and can provide

valuable input. The CCC will have the best grasp on what mitigation tools are in use today and can most efficiently recommend what tool(s) can best be used going forward. An example of a key area that has been discussed but not resolved, would be how low risk standard requirements can be moved to guidance (SER Phase II).

5. Is the multi-dimensional model shown in Figure 4 of the Whitepaper complete?

The Figure 4 model provides a conceptual view of when existing NERC tools will generally be employed based on risk timing and impact. For current purposes the model is generally complete. Currently, the model does not include dynamic forces outside of the ERO. As mentioned earlier there are risks that are not (completely) included in the purview of the Figure 4 model that can and will impact the timing and impact of risks. Going forward it should be noted the model leaves little room for change, or for new mitigation methods and for integration of mitigations shared with other industries.

NERC 3 Year Priorities

The Board requests policy input on the three most important reliability and security matters that NERC should address over the next three years. Chair Thilly put a finer point on the question during the MRC pre-meeting call saying that it would be the 3 issues that NERC should accomplish over the next three years. Below are 3 items (in no particular order) that the SM-TDU's believe NERC should address/accomplish over the next three years.

Improved Actionable Intelligence

Having actionable intelligence to ensure security is an issue that stakeholders believe needs to improve. Recent concerns such as the Executive Order on the Bulk Power System (BPS) and recent FERC Notice of Inquiries (NOIs) have highlighted this need.

The E-ISAC's revised business plan, as the SM-TDUs provided policy input in May 2020, is designed to improve the quality of the information provided to industry. SM-TDUs are encouraged by the plan as addressing this priority and look forward to its effective execution over the next three years.

Standards Efficiency Review

SM-TDUs believe that NERC should enhance staff resources on the Standards Efficiency Review (SER) project, including the review of the Critical Infrastructure Protection (CIP) standards. The Draft Standards Development Plan mentions Phase II and that it has been delayed by COVID-19. Stakeholders understand this delay, but still believe more could be done in the present that will provide significant efficiencies to improve ERO effectiveness over the next 3 years. Importantly, if NERC were to provide a comprehensive update of the achievements from the effort thus far and next steps, this would be valuable and appreciated by stakeholders.

A dedicated effort to transform standard requirements from administrative-based to results-based will allow registered entities and the ERO to increase focus on measurable security and reliability outcomes. Delaying the SER project also delays these efficiencies. SM-TDUs believe it is time to revitalize this work and that it should be accomplished as a priority as soon as possible.

ERO Assisting with Engagement with Third Party Suppliers

The risk associated with equipment and services from third parties has been highlighted by supply chain risk concerns. First, the risk was highlighted by the evolution of CIP-013. Registered

entities were concerned about their lack of leverage with suppliers, especially for smaller utilities. This concern became more complex when supply chain risk was associated with national adversaries. Cloud and virtualization technologies add another layer of complexity to the appropriate protocols for dealing with suppliers within the ERO regime. Stakeholders need NERC's assistance in bridging the gap with third parties to mitigate risk. Regardless of size, Registered Entities' leverage with suppliers is minimal, especially for smaller utilities, and ERO engagement and clarity will be key in alleviating the complexity of mitigating risks with third parties.