MEMORANDUM

TO: Suzanne Keenan,
Chair, NERC Board of Trustees

FROM: Roy Jones
Scott Tomashefsky
Tom Heller
Colin Hansen

DATE: June 2, 2026

The Sector 2 and 5 members of the North American Electric Reliability Corporation's (NERC) Members Representatives Committee (MRC), representing State/Municipal and Transmission Dependent Utilities (SM-TDUs), appreciate the opportunity to respond to your May 13, 2026, letter requesting MRC input on NERC's 2027–2029 planning and prioritization. Your letter asks for additional input as NERC develops more detailed execution plans, initiatives, and metrics to support the 2027–2029 Strategic Priorities and Goals. Specifically, your letter asks where NERC should prioritize or expand its focus to deliver the greatest reliability and security benefit, what efforts could be deferred or streamlined, how NERC can help industry manage the pace of change and cumulative workload, and how NERC can responsibly leverage emerging tools and technologies.

SM-TDUs appreciate NERC's engagement with industry generally, and with the MRC specifically, in developing the 2027–2029 Strategic Priorities and Goals. NERC's early and ongoing engagement with MRC members has been effective and constructive. We also appreciate the high level of engagement by the Board, NERC management, and NERC staff with Sectors 2 and 5. That engagement has improved significantly in recent years, and we value the positive working relationships that have developed with NERC leadership and staff.

As NERC moves from strategic priorities to implementation, we urge NERC to focus its efforts on the activities that produce the greatest incremental reliability and security benefit, while carefully considering cumulative industry workload, affordability, and the need to coordinate across the ERO Enterprise and with other governmental and industry partners.

SUMMARY OF COMMENTS

- NERC should prioritize activities that address higher-likelihood, higher-impact risks and should facilitate broader discussion about acceptable residual risk and the incremental value of different mitigation tools.
- NERC should improve analytical capabilities, particularly for gas-electric coordination and changing resource adequacy risks, while avoiding duplicative or inconsistent investments across NERC, Regional Entities, and industry.
- NERC should continue strengthening engagement with the electric industry. Expanded engagement with new or less-engaged stakeholders should complement—not replace—

continued engagement with Sectors 2 and 5 and other stakeholders with deep operational, planning, compliance, and governance experience.

- NERC should ensure that new technology investments, especially stakeholder-facing tools such as Modernization of Standards Processes and Procedures voting tools and compliance-related platforms, are informed by early stakeholder input, user-centered design, and robust testing before broad deployment.
- NERC and the E-ISAC should maximally leverage security work already being done by federal agencies, government-industry partnerships, Regional Entities, and private-sector security providers, and should avoid duplicative investments in new capabilities.

SM-TDU COMMENTS

NERC should prioritize activities that address higher-likelihood, higher-impact risks and should facilitate broader discussion about acceptable residual risk.

Your letter asks where NERC should prioritize or expand its focus to deliver the greatest reliability and security benefits. We believe NERC should prioritize the risks that are more likely to occur and more likely to produce material reliability or security consequences if they do occur. As NERC develops initiatives and metrics under the 2027–2029 plan, it should be clear about which risks warrant the greatest near-term attention and why.

NERC should also facilitate a broader conversation with stakeholders—possibly through the MRC or the Reliability Issues Steering Committee —about the treatment of residual risk within NERC and industry more broadly. We recognize that NERC is not seeking to eliminate *all* risk. The grid has always operated with some level of residual risk, and the objective of NERC's work is to reduce that risk effectively and efficiently. However, industry lacks a common vocabulary for discussing what degree of risk mitigation is sufficient, how much residual risk is acceptable, and when incremental mitigation no longer justifies the associated cost and workload.

That conversation matters for prioritization. NERC has many tools available to reduce risk and these tools impose different burdens and produce different levels of incremental risk reduction. When evaluating a new risk mitigation effort, NERC must consider not only how large the risk is, but also the *incremental* risk reduction of that effort compared to less burdensome options. For example, before moving an issue from a Level 3 Alert or other non-mandatory mechanism into a mandatory reliability standard, NERC should consider whether the additional risk reduction expected from mandatory enforceability justifies the additional industry workload, implementation costs, compliance obligations, and opportunity costs.

Mandatory reliability standards remain essential to bulk power system reliability. But prioritization should reflect a disciplined judgment about the incremental value of the mitigation tool selected. That discipline will help NERC focus limited resources on the activities most likely to improve reliability and security, while helping industry manage the cumulative workload associated with changing risks and risk mitigation activities.

NERC should improve analytical capabilities while avoiding duplicative or inconsistent investments across the ERO Enterprise and other industry entities.

We generally support NERC's plans to modernize reliability assessments and build improved analytical capabilities. Given the increasingly complex risk environment, NERC can provide significant value by improving the analytical tools, data quality, and assessment methods that support industry and policymaker understanding of those risks.

At the same time, NERC should ensure that investments in analytical capabilities are coordinated across the full ERO Enterprise and with other entities that are already making significant analytical investments. Many Regional Entities are strengthening their own analytical capabilities. Regional Transmission Organizations (RTOs), balancing authorities, planning coordinators, transmission planners, and state and regional organizations are also investing in modeling, scenario analysis, resource adequacy assessments, operational analytics, and gas-electric coordination tools. These efforts are important, but they create a risk of duplication, inconsistent assumptions, conflicting results, and unnecessary cost.

NERC—with the support of its standing committees— should therefore assess the broader analytical landscape before making major new investments. In some areas, NERC may be best positioned to conduct analysis directly; in others, NERC may add more value by coordinating work performed by Regional Entities, facilitating common assumptions, identifying gaps, improving transparency, or synthesizing analysis already being performed by RTOs, balancing authorities, and others. NERC should avoid building duplicative capabilities where existing regional or industry capabilities can be leveraged.

NERC should continue strengthening engagement with the electric industry while ensuring that expanded engagement complements existing stakeholder relationships.

We appreciate the Board's and NERC management's continued efforts to improve stakeholder engagement. NERC has engaged constructively with Sectors 2 and 5 on several significant issues over the past year. These engagements have been valuable, and they have strengthened the working relationships between NERC and our sectors. We especially note the added value of the quarterly trades meetings and the opportunities to engage with senior management and NERC Board members.

We also recognize that NERC is working to increase engagement with organizations and stakeholders that historically may not have had as much interaction with NERC – this effort is appropriate. The reliability and security issues facing the bulk power system increasingly affect a broader group of stakeholders, including policymakers, large loads, gas-sector entities, security partners, and others whose decisions can affect reliability outcomes.

But engagement is not a zero-sum exercise. Improving engagement with new stakeholders need not come at the expense of continuing to strengthen engagement with Sectors 2 and 5 and other stakeholders that have long participated in NERC processes. Sectors 2 and 5 include utilities with direct operational, planning, compliance, governance, and customer-facing responsibilities. Their perspectives are particularly important when NERC considers new standards, alerts, data requests, compliance processes, technology platforms, analytical tools, and security initiatives.

As NERC implements the 2027–2029 plan, it should continue improving the way it connects issues across programs and across stakeholder groups. NERC's work often spans multiple functions—standards, compliance, assessments, security, data collection, and external engagement. Each workstream is separate, but registered entities experience their cumulative effect. Stronger internal coordination within NERC and clearer external communications to industry would help stakeholders understand how individual initiatives fit together and how it is prioritizing among competing demands.

We also encourage NERC to continue providing early opportunities for stakeholder input before major proposals are substantially developed. Recent experience demonstrates that even where the underlying reliability issue is important, compressed comment periods can make it difficult for industry to provide the technical feedback needed to improve the final product. Early issue-framing discussions, transparent timelines, and meaningful opportunities for written and oral feedback can reduce the risk of avoidable controversy and improve the quality of NERC's work product.

NERC should ensure that new technology investments are informed by early stakeholder input, user-centered design, and robust testing.

Your letter asks whether NERC can thoughtfully and responsibly leverage emerging tools and technologies more aggressively in support of its reliability and security mission. We support responsible use of technology to improve NERC's effectiveness, reduce administrative burdens, and strengthen reliability and security outcomes. But as NERC invests in new tools during the 2027–2029 planning period, it should ensure that when tools are being used extensively by registered entities and other stakeholders, NERC should adopt user-centered design principles from the beginning.

Many NERC technology platforms are the mechanism through which registered entities provide information, respond to data requests, support audits, participate in standards development, vote on standards, and engage with NERC processes. When those tools are difficult to use, unclear, or insufficiently tested, the burden falls directly on registered entities and can distract from the underlying reliability objective.

Align and the Secure Evidence Locker provide well-known examples of technology platforms that are heavily used by registered entities but have faced challenges because they were not designed from the beginning to meet the needs of registered entities. Recent experience with data collection tools also illustrates the importance of usability. When data request forms include unclear questions, incorrect assumptions, or validation fields that prevent entities from entering accurate information, the problem is not merely administrative inconvenience. Poorly designed data collection tools can reduce the quality of the information NERC receives, increase burden on registered entities, create avoidable follow-up work for NERC staff, and undermine confidence in the process.

These problems can usually be avoided through early stakeholder review, plain-language testing of questions, pilot testing with a representative group of users, and validation testing before broad deployment.

This point is especially important for upcoming standards process modernization tools, including balloting and industry feedback tools. Those tools should be designed with direct input from the stakeholders who will use them, including representatives from different sectors, segments, organization sizes, and levels of NERC experience. NERC should test these tools before implementation, communicate clearly about how they will work, and provide opportunities for stakeholders to identify problems before the tools are used in consequential standards development activities.

NERC and the E-ISAC should leverage existing security work and avoid duplicative investments in new capabilities.

NERC's 2027–2029 plan appropriately identifies security as a major priority. Cybersecurity, physical security, supply chain risk, telecommunications risk, geopolitical threats, and hybrid threats all present significant challenges for the electric industry. We support NERC's continued efforts to improve industry resilience to security threats through threat detection, information sharing, partner collaboration, and response coordination.

At the same time, the security landscape is crowded. Many organizations already perform important work on grid security. Within the federal government, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response each have roles related to critical infrastructure security, cybersecurity, energy-sector resilience, emergency response, and threat information sharing. Government-industry partnerships, including the Electricity Subsector Coordinating Council and the Energy Threat Analysis Center, also support coordination between industry and government. Regional Entities conduct security-related outreach, compliance, assessments, and engagement. In addition, many utilities obtain security services, threat intelligence, assessments, and technical support from private-sector providers. Many smaller public power utilities also rely on programs supported by federal funding or partnerships to access security capabilities that would otherwise be difficult to obtain.

This broad ecosystem is valuable, but it also creates a risk of fragmentation and duplication. Utilities may receive similar requests, similar alerts, similar assessments, or similar recommendations from multiple organizations. New capabilities developed by one organization may overlap with tools or services already provided elsewhere. For smaller utilities in particular, navigating the number of security-related programs, information sources, exercises, and reporting expectations can be difficult.

The E-ISAC has an important role in this ecosystem, but it should not seek to duplicate the work of federal agencies, government-industry partnerships, Regional Entities, or private-sector providers. Instead, the E-ISAC should focus on where it can provide distinct value. Before making significant investments in new security capabilities, NERC and the E-ISAC should assess what capabilities already exist, where gaps remain, and whether NERC is best positioned to fill those gaps directly or to coordinate with others.

CONCLUSION

SM-TDUs appreciate the Board's continued engagement with the MRC and the opportunity to provide input as NERC develops more detailed execution plans for the 2027–2029 Strategic Priorities and Goals. NERC has identified the right broad categories of risk, and we support its efforts to improve reliability assessments, address emerging reliability and security risks, strengthen engagement, modernize processes, and responsibly leverage technology. As NERC moves from strategy to implementation, we urge the Board and NERC management to apply disciplined prioritization.

We look forward to continued collaboration with the Board, NERC management, NERC staff, the Regional Entities, and other industry stakeholders in support of our shared goal of assuring the reliability and security of the bulk power system.