MEMORANDUM

TO: Kristen Iwanechko, Secretary
NERC Member Representatives Committee

FROM: Allen Mosher, Vice President, Policy Analysis, American Public Power Association
Jacqueline Sargent, General Manager, Platte River Power Authority, on behalf of the Large Public Power Council
John Twitty, Executive Director, Transmission Access Policy Study Group

DATE: April 29, 2014

SUBJECT: Response to Request for Policy Input

The American Public Power Association, the Large Public Power Council, and the 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 Fred W. Gorbet's April 9, 2014 letter requesting policy input in advance of the May 2014 NERC Board of Trustees meeting.

MEMORANDUM

TO: Kristin Iwanechko, Secretary
NERC Member Representatives Committee

FROM: Carol Chinn
Jackie Sargent
Bill Gallagher
John Twitty

DATE: April 29, 2014

SUBJECT: Response to Request for Policy Input

The MRC's State/Municipal and Transmission Dependent Utility sectors ("SM-TDUs") appreciate the opportunity to respond to the April 9, 2014 letter from NERC Board Chair Fred W. Gorbet to Mr. John A. Anderson, Chair of the NERC Member Representatives Committee ("MRC"), requesting policy input on topics that will be of particular interest during the upcoming May 6-7, 2014 meetings of the NERC Board of Trustees, Board committees, and NERC MRC.

This response is divided into two parts. Part one outlines our strong support for NERC's efforts on many fronts to ensure the physical and cyber security of the electricity sector in North America and reiterates our full support for a government-industry partnership that combines NERC reliability standards with information sharing and analysis, coordination, contingency planning and exercises to increase the resiliency of the nation's critical infrastructures. We commend in particular NERC's response to the Commission's order directing NERC to submit a physical security reliability standard on or before June 5, 2014 and NERC's efforts through the Electricity Sector Information Sharing and Analysis Center ("ES-ISAC") to alert the industry on the Heartbleed cybersecurity vulnerability.

Part two addresses each of the three items specifically identified in Mr. Gorbet's letter: the Reliability Standard Audit Worksheet ("RSAW") review and revision process, the Risk-Based Registration Initiative, and Potential Alternative Funding Mechanisms to Support Expanded Cyber Security Information Sharing and Associated Capabilities. To summarize our views:

- SM-TDUs support the proposed RSAW review and revision process and urge NERC to codify procedures that ensure consistency and quality in the revision process.

- We fully support NERC's Risk-Based Registration Initiative as a long-overdue effort to "right-size" the NERC compliance registry to include only those entities that have a material impact on bulk electric system reliability, while ensuring that this reform creates no material gaps in NERC's reliability programs.

- We strongly support expanded funding for and enhanced capabilities for the NERC ES-ISAC – and including that funding within NERC's section 215 Business Plan and Budget and annual assessments to load-serving entities. All electricity sector entities in North

America benefit tangibly from NERC's efforts on this front, even when they do not participate directly in the ES-ISAC, because these efforts serve to increase the resiliency of the entire sector. If and when NERC or the ES-ISAC undertake analytical projects that do not provide broad benefits to the electricity sector as a whole, these costs can and should be directly assigned to the beneficiaries, with the revenues received credited to operating reserves, thereby reducing next year's NERC budget assessment.

As a final note on SM-TDU's broader policy concerns, we urge the Board to press NERC staff and the regions to complete their work on the Reliability Assurance Initiative's design and bring the field trials to conclusion. RAI needs to be brought to implementation in a form that is actionable by and beneficial to registered entities.

I. Physical and Cyber Security of the Electricity Sector

NERC and the industry as a whole have been subject to recent criticisms of our efforts to ensure the physical and cyber security and resiliency of the electricity sector in the United States and elsewhere in North America. Some have taken the occasion of the Metcalf attack to level charges that the industry seemingly does not care about physical security and to assert that the section 215 regulatory model, with an independent Electric Reliability Organization certified by the Federal Energy Regulatory Commission, is somehow structurally deficient.

SM-TDUs disagree with these criticisms. As Sue Kelly, president and CEO of the American Public Power Association testified before the Senate Energy and Natural Resources Committee on April 10, 2014, the reliability of the bulk electric system — "keeping the lights on" for our customers and the economy — is a national security issue. And it is of paramount importance to electric utilities. Industry for decades has taken action to protect the grid and is now working closely with government officials to continue to keep it safe.

When it comes to physical security threats, utilities have routinely deployed risk mitigation measures, such as cameras and locks. We are now going further, employing "defense-in-depth" techniques, to reinforce and strengthen security measures that will protect our facilities and allow the grid to recover quickly if an attack should occur. But since there are over 45,000 substations in the United States, prioritizing resources to protect the most critical assets is crucial.

We are moving forward through partnerships with government officials at all levels. After the Metcalf incident, government and industry conducted a series of briefings across the country for utilities and local law enforcement to learn more about it and how best to respond. These information sharing activities continue at the federal, state and local levels.

Also, on March 7, the Federal Energy Regulatory Commission (FERC) directed NERC to submit proposed physical security standards covering critical assets within 90 days. NERC has moved with alacrity, achieving super-majority support for the first draft of the standards less than 50 days later. SM-TDUs are confident that a final version of the proposed standard will be presented to the independent NERC Board of Trustees for adoption in late May, for timely submission to the Commission.

Cybersecurity entails a similar multi-level response, which includes taking an enterprise-wide perspective on cybersecurity within each of our utilities, deployment of advanced detection and protection tools, information sharing with our government partners, preparation for cyber events, and the application of cybersecurity standards to our bulk electric system operations through NERC's Critical Infrastructure Protection standards.

The recent disclosure of the "Heartbleed" vulnerability is a case in point. NERC's initial Industry Advisory was distributed on April 11, just days after public disclosure of the vulnerability in the OpenSSL encryption library, followed soon after by an industry-wide webinar describing steps that electric utilities can take to identify and assess their specific vulnerabilities and patch them expeditiously. SM-TDUs commend NERC for performing the pivotal task of ensuring timely communication of emerging threats and vulnerabilities to the industry.

To summarize, grid security requires collaboration: it is, and must be, a shared responsibility between industry, NERC and government. Our industry is investing in security measures to protect the grid against evolving threats and make it more resilient and robust. With the help of government, the entire electric utility industry will work to protect critical electric utility infrastructure from both cyber and physical threats. NERC fills a pivotal role in this process.

II. Policy Input Topics

A. Reliability Standard Audit Worksheet (RSAW) Review and Revision Process

SM-TDUs are highly supportive of the proposed Reliability Standards Audit Worksheet (RSAW) review and revision process. This simple process memorializes the essence of a key Standards Process Input Group (SPIG) recommendation that was endorsed by the BOT in 2012.

RSAWs are a critical tool for the ERO and registered entities. This tool outlines compliance expectations for registered entities and guidance for auditors in the compliance monitoring and enforcement process.

We are encouraged that RSAWs are now posted alongside balloted standards. Clearly the revision process must also be just as transparent. Providing regulatory certainty is a core accountability for the ERO and we view the RSAW review and revision process as a good control in assuring regulatory certainty. The timely development and posting of RSAWs is a key element to gaining stakeholder consensus in support of new and revised reliability standards.

On a related note, currently there are some highly complex standards that are lacking an RSAW, including PRC-005-2, TPL-001-4 and CIP Version 5. While these standards are each subject to future enforcement, registered entities are already in the implementation stage and need the RSAWs to assure compliance.

We appreciate that the Board had been very supportive of a strong emphasis on RSAWs. Having Board representation on the SPIG back in 2012 and now with representation on this recent MRC RSAW working group, we are making good strides in improving the clarity and consistency of compliance expectations.

B. Risk-Based Registration Initiative

SM-TDUs fully support NERC's Risk-Based Registration Initiative as a long-overdue effort to "right-size" the NERC compliance registry to include only those entities that have a material impact on bulk electric system reliability, while ensuring that this reform creates no material gaps in NERC's reliability programs.

The current registration paradigm is out of step with NERC's ongoing efforts to align standards, compliance, and enforcement with risk to the grid. Many of the nearly 2000 entities on the NERC Compliance Registry pose little to no risk to the Bulk Electric System ("BES"), or are subject to demonstrating compliance with requirements far in excess of what is needed to protect the BES and ensure reliable operations. To make matters worse, the NERC Rules of Procedure lack clear deregistration procedures and timelines, leaving entities that are over-registered under the current registry criteria subject to compliance while their deregistration requests remain in limbo. This situation is inefficient, burdensome, and reflects an outdated, one-size-fits-all approach to registration, standards and compliance that is incompatible with the risk-informed focus that NERC seeks to bring to all of its activities.

Tailoring entities' compliance responsibilities to their impact on the grid will relieve some small entities from NERC compliance burdens altogether, reduce the burden on others through more targeted applicability, and save significant resources for all involved, thereby allowing the industry and the ERO enterprise to enhance reliability by focusing their resources on material risks to reliability. And with the upcoming implementation of the revised BES definition, the time is right to reform the registry to reflect risk.

SM-TDUs support the priority afforded to this initiative, including the commitment to present a new registration framework and transition plan at the November 2014 Board of Trustees meeting. The project plan is ambitious but achievable, because many promising approaches can be used in combination to achieve a risk-based approach to registration. These approaches include:

- Incorporating the revised definition of Bulk Electric System into the design and implementation of the NERC Statement of Compliance Registry Criteria, to align registration, standards applicability and compliance with the BES' bright line criteria and application of the BES exception process.

- Increasing the size thresholds or adding new refining criteria to limit registration of entities that do not perform core BES reliability functions, particularly small DPs and LSEs that do not own required BES protection systems;

- Targeting the applicability of reliability standards applicable to small GOs and GOPs that are shown to have only limited capability to support reliable BES operations;

- Using the successful GO-TO model to address the limited BES reliability impacts of DPs with limited BES transmission elements, by extending the applicability of certain standards to such DPs, rather than registering such entities as TO/TOPs;

- Eliminating altogether the registration of entities that perform largely commercial functions and do not have a material impact on BES reliability, such as PSEs and IAs;

- Codifying improved procedures for deregistration of entities that do not meet the revised registration criteria, as well as for procedures (similar to the BES exception process) for case-by-case resolution of requests to register or deregister a particular entity where the revised registry criteria fail to accurately reflect its impact on BES reliability;

- Clarifying evidentiary requirements to make showings of material impact on the BES and aligning the technical foundation for material impact with NERC reliability standards and the assessment of risks to the BES; and

- Developing the NERC enterprise-wide business processes and infrastructure to carry out the Risk-Based Registration Initiative.

SM-TDUs urge the Board to endorse this important initiative and ensure that NERC staff has the resources necessary to meet the proposed deadlines.

C. Potential Alternative Funding Mechanisms to Support Expanded Cyber Security Information Sharing and Associated Capabilities

SM-TDUs strongly support expanded funding for and enhanced capabilities for the NERC ES-ISAC – and including that funding within NERC's section 215 Business Plan and Budget and annual assessments to load-serving entities. All electricity sector entities in North America benefit tangibly from NERC's efforts on this front, even when they do not participate directly in the ES-ISAC, because these efforts serve to increase the resiliency of the entire sector.

A good example of these efforts is NERC's support for the Cybersecurity Risk Information Sharing Program (CRISP), an initiative by the U.S. Department of Energy to deploy information sharing devices (ISDs) within the electric utility industry at the cyber interface between each participating utility's external and internal systems, to analyze IT traffic flows for hostile digital signatures. The CRISP system includes a sophisticated, encryption-based information exchange protocol, the Cyber Federated Model (CFM), which allows the site to specifically determine who receives its data. Along with reports, and other situational-analysis information generated through CRISP, the data shared is a combination of hostile IP addresses, DNS domains, and other indicators. Each of the participating utilities will bear the direct costs of installing the ISDs and will share the ongoing contractor costs of analyzing the information flows. The NERC ES-ISAC will perform an equally important but different role: taking the results of these analyses and working with the contractor to anonymize the resulting indicators of threats and vulnerabilities, to develop alerts and advisories that can be shared with the electricity sector as a whole. Anonymized information may also be shared with the federal government and the ISACs for other critical infrastructure sectors.

SM-TDUs view such activities to be fully consistent with NERC's role as the Electric Reliability Organization for North America, charged with ensuring the reliable operation of the bulk-power system. The NERC budget is an equitable approach for funding the ES-ISAC, including these new initiatives. While a small percentage of the ES-ISAC's participants are not on the NERC

compliance registry, each such entity is paying its load ratio share of NERC's budget, including the ES-ISAC. If and when NERC or the ES-ISAC undertake analytical projects that do not provide broad benefits to the electricity sector as a whole, these costs can and should be directly assigned to the beneficiaries, with the revenues received credited to NERC's operating reserves, thereby reducing next year's NERC budget assessment on load-serving entities.

The NERC Board, stakeholders and regulatory authorities have an obligation to review, comment on and approve the NERC Business Plan and Budget, including the ES-ISAC. At some juncture, NERC may propose to undertake projects within the ES-ISAC that we may oppose, because such projects are inappropriate for NERC, excessively costly, or better performed by other organizations. SM-TDUs will undertake such due diligence when the proposed 2015 Business Plan and Budget is posted on May 16.

Thank you for the opportunity to provide this policy input.