December 23, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

RE: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick:

Tri-State Generation and Transmission Association Inc. ("Tri-State") appreciates the opportunity to submit these comments to the National Institute of Standards and Technology ("NIST") for its consideration in the development of the Cybersecurity Framework set to be finalized in February 2014 at the direction of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." Tri-State respectfully requests that its out-of-time comments be considered noting the comments are provided to further support and build upon the comments submitted by the National Rural Electric Cooperative Association ("NRECA"), in conjunction with several other energy trade associations, on December 13, 2013. Tri-State's comments are limited in focus and address one issue regarding the seeming overlap of the NIST Cybersecurity Framework with respect to the energy industry and the existing North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Reliability Standards. As an owner and operator of critical infrastructure, as defined by Executive Order 13636, Tri-State's interests will be directly affected by this proceeding. Given that the final Cybersecurity Framework is not set to be published until February 2014, Tri-State submits that permitting its comments out-of-time will not disrupt NIST's Framework development efforts nor cause disruption or inconvenience to any other party.

All correspondence and communications to Tri-State regarding these comments should be addressed to:

Luis A. Zaragoza, CPA
Senior Manager-Corporate Compliance
Tri-State Generation and Transmission
Association Inc.
1100 W. 116th Avenue
Westminster, Colorado 80234
Telephone: (303) 254-3113
E-mail: lzaragoza@tristategt.org

Timothy Woolley
Assistant General Counsel-Regulatory Affairs
Tri-State Generation and Transmission
Association Inc.
1100 W. 116th Avenue
Westminster, Colorado 80234
Telephone: (303) 254-3277
E-mail: twoolley@tristategt.org

Kristen Connolly McCullough
Natalie M. Karas
Duncan, Weinberg, Genzer & Pembroke, P.C.
1615 M Street, NW
Suite 800
Washington, DC 20036
Telephone: (202) 467-6370
E-mail: kc@dwgp.com
nmk@dwgp.com

and

Sean M. Neal
Duncan, Weinberg, Genzer & Pembroke, P.C.
915 L Street
Suite 1410
Sacramento, CA 95814
Telephone: (916) 498-0121
E-mail: smn@dwgp.com

Tri-State is a cooperative corporation headquartered in Westminster, Colorado. Tri-State's primary functions involve the generation, transmission, transformation and sale of electricity at wholesale to its 44 member-owner distribution cooperatives within the states of Colorado, Nebraska, New Mexico and Wyoming. Tri-State operates in five Balancing Area Authorities: PacifiCorp, Public Service Company of Colorado, the Western Area Power Administration, the Nebraska Public Power District and Public Service Company of New Mexico. The member systems serve approximately 1.4 million consumers with load in both the Western and Eastern Interconnections.

Tri-State has outstanding debt with the U.S. Department of Agriculture's Rural Utilities Service and therefore is not a "public utility" as that term is defined in Section 201(e) of the Federal Power Act.[1] Tri-State is included on the NERC compliance registry for multiple functions. As a result, Tri-State is subject to all applicable NERC Reliability Standards, including the CIP Reliability Standards. Accordingly, Tri-State has a direct and substantial interest in this

[1] 16 U.S.C. § 824(e).

proceeding to the extent that the Preliminary Cybersecurity Framework may ultimately lead to duplicative or new critical infrastructure protection and cybersecurity standards that may not result in any additional security than that already provided for by the NERC CIP Reliability Standards.

These comments address Tri-State's concern that the NIST Cybersecurity Framework potentially creates greater burdens on the energy industry over and above the NERC Reliability Standards that will not lead to greater gains in cybersecurity reliability. Tri-State also has concerns that what is developed in a voluntary framework will become incorporated into the mandatory and enforceable regime of the NERC CIP Reliability Standards. While Tri-State supports efforts to improve reliability and minimize cybersecurity risk impacting the bulk-power system, Tri-State is concerned that the application of guidelines and frameworks created in a voluntary context to the existing NERC regime may have unintended consequences for the users, owners and operators of the bulk-power system subject to up to $1 million penalties per day for each instance of NERC Reliability Standard Requirement violations.[2]

The voluntary NIST Cybersecurity Framework is intended to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" based on "existing standards, guidance, and best practices to achieve outcomes that can assist organizations responsible for critical infrastructure services to manage cybersecurity risk."[3] Notably, the broad scope of the Executive Order and the NIST Preliminary Cybersecurity Framework encompasses all organizations responsible for critical infrastructure services to manage cybersecurity risk, and is not limited to the electric industry. Per the Executive Order, "critical infrastructure" is broadly defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters."[4]

While the Preliminary Cybersecurity Framework suggests that the voluntary "Framework complements, and does not replace, an organization's existing business or cybersecurity risk management process and cybersecurity program," Tri-State believes it adds an unnecessary, additional layer of complexity for the electric industry to consider and incorporate because it is already subject to and implementing mandatory and enforceable NERC CIP Reliability Standards. The electric industry, unlike other critical infrastructure subject to the NIST Cybersecurity Framework, is already regulated by the Federal Energy Regulatory Commission

---

2 *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104 at P 575(2006) (finding that section 316A of the Federal Power Act establishes a limit on a monetary penalty for a violation of a Reliability Standard that may be imposed by the Federal Energy Regulatory Commission, the Electric Reliability Organization (*i.e.*, NERC), or a Regional Entity pursuant to section 215 of the Federal Power Act.

3 Preliminary Cybersecurity Framework at 1.

4 *Id.*

and NERC. Through section 215 of the Federal Power Act, 16 U.S.C. 824o, the Federal Energy Regulatory Commission and NERC oversee the establishment and enforcement of Reliability Standards, ensure cybersecurity protection (section 215(a)(3)), and ensure the reliable operation of the bulk-power system in the event of cybersecurity incidents (section 215(a)(4)).

Tri-State notes that the first bulleted point in the December 13, 2013 comments submitted by NRECA and the other energy trade associations provides that "Section 3.0 of the Framework should support sector-level coordination to develop implementation guidance." In those comments, NRECA and the energy trade associations request that NIST encourage the sectors to coordinate with their Sector-Specific Agencies to review the Cybersecurity Framework and develop implementation guidance to integrate existing and future efforts in order to enable the Energy Sector to leverage and integrate cybersecurity improvements already underway into the Framework. NRECA and the energy trade associations reason (at 2) that because members of the energy sector "have already devoted significant resources towards reducing cyber risk," NIST's support of sector-level coordination to develop implementation guidance is critical to the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure in the energy sector.

While Tri-State agrees with the concern being addressed by the energy trade associations' proposed solution, Tri-State offers a different solution. Tri-State urges NIST to remove the energy sector from the scope of the general, voluntary Cybersecurity Framework in recognition of the energy sector's ongoing efforts to minimize cybersecurity threats to the critical infrastructure of the bulk-power system and of the existing NERC Reliability Standards. Because the energy sector is already subject to mandatory and enforceable CIP Reliability Standards, any further efforts to alleviate cybersecurity risk pursuant to the Executive Order should occur only pursuant to the consultative process outlined in Section 6 of the Executive Order.[5] According to the written testimony before the U.S. House of Representatives Energy and Commerce Committee's Subcommittee on Energy and Power on December 5, 2013 (at 3-4) of Cheryl LaFleur, Acting Chairman of the Federal Energy Regulatory Commission, the Federal Energy Regulatory Commission and NIST are already participating in such a consultative process. Tri-State supports this consultative process between NIST and the Federal Energy Regulatory Commission, as well as NERC.

While the Framework is voluntary and generically applies to all critical infrastructures, not just energy, the concern is that the new Framework might create a new guideline that could lead to duplicative or supplemental requirements that do not add any further protections to those already required in the NERC Reliability Standards. Until now, NIST has, by and large, focused on securing the confidentiality of data and protecting information systems, not the industrial control

---

[5] Section 6 of the Executive Order states: "The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts."

systems underlying the reliability of the bulk electric system. The NERC CIP Reliability Standards focus on a relatively small number of reliability services that need to be protected as opposed to the NIST mission of establishing general standards across the board for many organizations with vastly different missions. Encouraging the energy sector to adopt or determine how to integrate an overly broad Cybersecurity Framework would further add to the regulatory burdens on an energy sector with finite resources without any assurance that any additional cybersecurity benefits would be achieved.

An important caveat is made explicit in the NIST Preliminary Cybersecurity Framework: "The Framework complements, and does not replace, an organization's existing business or cybersecurity risk management process and cybersecurity program." *Id.* at 2. The intended "complementary" nature of the Framework to the NERC CIP Reliability Standards compliance efforts by the energy industry is the cause of Tri-State's concern. Tri-State notes the relationship between the NIST Preliminary Framework and the CIP Reliability Standards is inevitably linked given the Federal Energy Regulatory Commission's precedent of directing NERC to review and incorporate NIST standards and frameworks into the development of the CIP Reliability Standards. For example, in the order approving the original CIP Reliability Standards in 2008, the Federal Energy Regulatory Commission concluded:

> The Commission continues to believe – and is further persuaded by the comments – that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the [NERC, as the Electric Reliability Organization] to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.[6]

The Federal Energy Regulatory Commission continues to direct NERC to review and consider NIST developments as NERC pursues its obligations pursuant to section 215 of the Federal Power Act. The Federal Energy Regulatory Commission continues to use NIST frameworks and policies as a basis for comparison and a baseline for NERC standards to strive to meet. When NERC submitted the latest iteration of the CIP Reliability Standards (Version 5) to the Federal Energy Regulatory Commission for approval, NERC noted the modified standards incorporated aspects of NIST's frameworks and policies after a careful review in the NERC Reliability

---

[6] *Mandatory Reliability Standards for Critical Infrastructure Protection,* Order No. 706, 122 FERC ¶ 61,040 at P 233 (2008) (footnote omitted).

Standards development process. In the Federal Energy Regulatory Commission's notice of proposed rulemaking regarding these Version 5 CIP Reliability Standards, however, the Commission pointed out that NERC's proposed categorization process is based on facility ratings, such as generation capacity and voltage levels, whereas the NIST Risk Management Framework categorizes systems based on cyber security principles regarding the confidentiality, integrity, and availability of systems.[7] The Federal Energy Regulatory Commission also sought comment on "whether, and in what way, adoption of certain [other] aspects of the NIST Risk Management Framework could improve the security controls proposed in the CIP version 5 Standards."[8] In its comments in response to the notice of proposed rulemaking, NERC proffered it is a discussion for a technical forum inclusive of industry, NERC, and Commission staff with respect to whether or how to incorporate additional elements of the NIST Risk Management Framework (and any other NIST standards) in the CIP Reliability Standards.[9] Tri-State agrees that NERC appropriately modified NIST standards when integrating them into the CIP Reliability Standards with respect to the relevant categorization process for the identification of assets for protection. Tri-State adds that it is not beneficial to have the all-encompassing NIST Frameworks applicable to the energy sector when NERC and the Federal Energy Regulatory Commission have been specifically authorized to develop and enforce Reliability Standards tailored to protect the reliability of the bulk-power system, including with respect to cybersecurity incidents.[10]

The Federal Energy Regulatory Commission agreed with the approach proposed by NERC that a technical conference discussing certain technical issues and the relevance of the NIST Risk Management Framework to the CIP Reliability Standards was an appropriate next step, rather than directing NERC to simply adopt NIST's guidelines wholesale.[11] Tri-State submits that this example of the historical practice of leaving it to NERC to determine how best to incorporate NIST standards into the CIP Reliability Standards should continue. NERC and the energy industry through the NERC Reliability Standards development process should have the opportunity to review and analyze what is developed in a broader context by NIST and determine if it is appropriate to incorporate into the CIP Reliability Standards (and how best this may be done). Tri-State believes the same approach is appropriate with respect to NIST's Cybersecurity Framework.

The subject matter of the NIST Cybersecurity Framework is already the responsibility of NERC, the Electric Reliability Organization certified by the Federal Energy Regulatory Commission, pursuant to section 215(c) of the Federal Power Act. As the Electric Reliability Organization, NERC has been certified to establish and enforce reliability standards for the bulk-power

---

7 *Version 5 Critical Infrastructure Protection Reliability Standards,* NOPR, 143 FERC ¶ 61,055 at P 61 (2013) ("Version 5 CIP NOPR").

8 *Id.* at P 117.

9 *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 at P 221 (2013) ("Order 791").

10 *See* section 215(a)(3) of the Federal Power Act.

11 *Order 791* at P 225.

system.[12] The statute defines a reliability standard as a requirement, approved by the Federal Energy Regulatory Commission, to provide for reliable operation of the bulk-power system, including cybersecurity protection.[13] The reliable operation intended to be achieved by the implementation of the reliability standards includes the avoidance of instability, uncontrolled separation, or cascading failures as a result of a cybersecurity incident.[14] Section 215(a)(8) of the Federal Power Act defines a "cybersecurity incident" as "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system." Clearly, it is within NERC's purview to develop cybersecurity standards to protect the critical infrastructure of the bulk-power system. Likewise, historical practice indicates that NERC reviews and incorporates appropriate elements of NIST-developed guidelines and frameworks into the NERC-proposed Reliability Standards.

Notably, Congress has previously ensured that NERC and the energy industry are heavily involved in the development of standards for the protection of the cyber risks associated with the energy critical infrastructure, which includes the consideration of whether any NIST-developed guidelines and frameworks are appropriately adopted in CIP Reliability Standards. *See generally* section 215 of the Federal Power Act. NERC must have rules that provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties.[15] And, unlike other provisions of the Federal Power Act, the Federal Energy Regulatory Commission may not unilaterally revise what is submitted to it in a filing as NERC retains control of the development of reliability standards. Section 215(d)(4) of the Federal Power Act provides that the Federal Energy Regulatory Commission shall remand to NERC for further consideration a proposed reliability standard or a modification to a reliability standard that the Commission disapproves in whole or in part.

In the context of the critical infrastructure of the bulk-power system, a technically knowledgeable, sector-specific certified Electric Reliability Organization has the authority to ensure the reliable operation and cybersecurity protection of the bulk-power system through a Reliability Standards development process that heavily relies upon those with intimate knowledge of the critical infrastructure to be protected (*i.e.*, the users, owners and operators of the bulk-power system). Congress chose not to place exclusive authority at the Federal Energy Regulatory Commission or implement any other top-down approach to developing cybersecurity protections for the bulk-power system, instead opting to create an Electric Reliability Organization and specifying requirements that standards be developed in consultation with the industry.[16] Given the structure outlined in section 215 of the Federal Power Act for the development of applicable cybersecurity reliability standards, it is not appropriate for the NIST

---

12 Section 215(a)(2) of the Federal Power Act.

13 Section 215(a)(3) of the Federal Power Act.

14 Section 215(a)(4) of the Federal Power Act.

15 Section 215(c)(2)(D) of the Federal Power Act.

16 *See id*.

Cybersecurity Framework to be thrust upon the Energy Sector without following the controls provided in the Federal Power Act and being funneled through the technical expertise of NERC and the Reliability Standards development process for any necessary tailoring.

In sum, Tri-State urges NIST to continue to work in a consultative process with the Federal Energy Regulatory Commission and NERC to assist in the development of a cybersecurity framework. However, these efforts should be distinct from any effort to unilaterally impose a Cybersecurity Framework developed in a general and voluntary context onto the electricity sector that is already subject to mandatory and enforceable CIP Reliability Standards with an existing process to tailor any appropriate elements for incorporation into the NERC Reliability Standards after a careful review and vetting of the Cybersecurity Framework.

Tri-State respectfully requests consideration of these comments as NIST finalizes the Cybersecurity Framework.

Sincerely,

/s/ Kristen Connolly McCullough

Kristen Connolly McCullough
Duncan, Weinberg, Genzer &
Pembroke, P.C.
1615 M Street, NW, Suite 800
Washington, DC 20036-3203
(202) 467-6370
(202) 467-6379 (facsimile)
kc@dwgp.com

Attorney for Tri-State Generation
and Transmission Association Inc.