UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Version 5 Critical Infrastructure Protection Reliability Standards	Docket No. RM13-5-000

COMMENTS OF TRANSMISSION ACCESS POLICY STUDY GROUP

Pursuant to the Commission's April 18, 2013 Notice of Proposed Rulemaking ("NOPR"),[1] the Transmission Access Policy Study Group ("TAPS") comments on the NOPR's proposal to approve, with directives, the Version 5 Critical Infrastructure Protection Reliability Standards ("CIP v5 Standards") submitted by the North American Electric Reliability Corporation ("NERC").

TAPS supports the CIP v5 Standards and the associated implementation plan, as proposed by NERC. We do not support any directives to modify the standards. In particular, we request that the Commission not adopt the NOPR's proposed directive to impose specific cyber security controls for Low Impact cyber systems, but instead accept NERC's proposal to require implementation of cyber security policies for those low impact systems. If the Final Rule does direct modifications on Low Impact cyber systems, TAPS urges the Commission to allow NERC the flexibility to redefine or further subdivide the Low Impact category as part of NERC's efforts to develop an equally efficient or superior solution to the Commission's concerns.

---

[1] *Version 5 Critical Infrastructure Protection Reliability Standards*, 143 FERC ¶ 61,055 (2013).

I. INTERESTS OF TAPS

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states, promoting open and non-discriminatory transmission access.[2] As transmission-dependent utilities, TAPS members have long recognized the importance of grid reliability. As TDUs, TAPS members are users of the Bulk-Power System, highly reliant on the reliability of facilities owned and operated by others for the transmission service required to meet TAPS members' loads. In addition, many TAPS members participate in the development of and are subject to compliance with NERC Reliability Standards. Thus, TAPS is sensitive to both the need for standards to support grid reliability, as well as the need to make the standards clear and cost-effective.

Communications regarding these proceedings should be directed to:

John Twitty
Executive Director
TAPS
4203 E. Woodland St.
Springfield, MO 65809
Tel.: (417) 838-8576
E-mail: 835consulting@gmail.com

Cynthia S. Bogorad
Rebecca J. Baldwin
Latif M. Nurani
SPIEGEL & MCDIARMID LLP
1333 New Hampshire Ave., NW
Washington, DC 20036
Tel.: (202) 879-4000
Fax: (202) 393-2866
E-mail: cynthia.bogorad@spiegelmcd.com
rebecca.baldwin@spiegelmcd.com
latif.nurani@spiegelmcd.com

II. COMMENTS

A. TAPS supports the CIP v5 Standards and the associated implementation plan as filed by NERC

TAPS supports the CIP v5 Standards as filed by NERC. NERC's proposed standards represent a reasonable approach to securing the Bulk-Power System against

---

[2] Tom Heller, Missouri River Energy Services, chairs the TAPS Board. Cindy Holman, Oklahoma Municipal Power Authority, is TAPS' Vice Chair. John Twitty is TAPS' Executive Director.

cyber threats and implementing outstanding Commission directives. The Commission should therefore approve the CIP v5 Standards without directing any modifications. As discussed below, TAPS opposes the NOPR's proposed directive to impose specific cyber controls on Low Impact cyber systems. Although our comments focus on the standards applicable to Low Impact cyber systems (which is likely to be the category in which the bulk of the cyber assets of TAPS members fall), TAPS does not support any of the NOPR's contemplated directives to modify the CIP v5 Standards.

TAPS supports NERC's implementation plan, and the NOPR's proposal to approve that plan without change. The implementation plan would allow responsible entities to transition directly from compliance with the currently effective CIP v3 Standards to compliance with the CIP v5 Standards. The implementation plan will avoid unnecessary work to prepare for the CIP v4 Standards, allowing registered entities to focus limited resources on improving reliability.

B. NERC's proposal for Low Impact systems should be accepted without modification

1. CIP v5's inclusion of Low Impact cyber systems is just and reasonable and in the public interest

NERC has proposed requiring responsible entities to categorize all BES Cyber Systems as having a Low, Medium, or High Impact. Low Impact cyber systems are defined as all BES Cyber Systems that are not classified as either Medium or High Impact; thus all BES Cyber Systems will have a minimum classification of Low Impact. NERC would require owners of Low Impact cyber systems to implement "documented

cyber security policies"[3] for those systems, but would not mandate a set of specific controls applicable to all Low Impact assets.

NERC's proposal for Low Impact systems should be accepted without modification, because it reasonably expands the scope of the CIP standards while allowing responsible entities the flexibility to develop and implement cyber policies designed to protect those Low Impact systems. Under CIP v5, many assets that were not covered by earlier versions of the CIP standards will now be covered by mandatory standards. The Low Impact category is a catch-all that includes a wide range of BES Cyber Systems that are not categorized as Medium or High Impact. Thus, the Low Impact category is likely to include many more assets than the Medium or High Impact categories. Not only will the Low Impact category include *more* assets than the other categories, but it will also include *more diverse* assets. On one end of the spectrum, it could include a single microprocessor-based protective relay. On the other end of the spectrum, it could include control systems for small generators along with associated control rooms and computer equipment.

Given the large number of assets that will be included in the Low Impact category, and the diversity of those assets, NERC prudently proposed a standard that would allow responsible entities to develop and implement tailored policies to protect the various classes of Low Impact cyber systems. Those policies will address cyber security awareness, physical security controls, electronic access controls, and incident response. This mandatory standard would require responsible entities not just to have a plan on paper, but also to implement that plan to protect its assets.

---

[3] NOPR, P 5.

Thus, the CIP v5 Standards, as filed by NERC, amply satisfy the statutory requirement that standards be found just and reasonable and in the public interest.[4] The Commission should approve, without modification, NERC's proposal to require development and implementation of cyber security policies for Low Impact cyber systems.

2. Implementing common cyber security controls for all Low Impact cyber systems will not improve reliability

The NOPR expresses concern that NERC's proposal will result in ambiguity and may lead to inconsistent and inefficient implementation of the CIP Reliability Standards with regard to Low Impact cyber systems. The NOPR therefore proposes to direct NERC to require responsible entities to adopt specific, technically supported cyber security controls for Low Impact assets.[5] The Commission should not adopt the NOPR's proposed directive.

Given the broad diversity of Low Impact cyber systems, it is not practical to dictate a single set of controls that would apply to all assets in the Low Impact category. Such a one-size-fits-all approach risks imposing inappropriate controls on different classes of Low Impact assets. Especially considering that these assets have, by definition, lower impact on the reliability of the BES, the burden of complying with poorly tailored requirements could detract from implementing effective reliability policies for specific cyber systems. Moreover, many of the assets that will be included in the Low Impact category have never been subject to CIP standards before, which makes it even more difficult to impose appropriate controls at this time.

---

[4] 16 U.S.C. § 824*o*(d)(2).

[5] NOPR, P 70.

The NOPR's proposed directive could be counterproductive. Although specific controls are valuable tools to protect reliability—they are easy to enforce and they provide for a minimum level of performance—specific controls also have a cost: they reduce flexibility and risk inhibiting creativity. In the case of Low Impact systems, which are both more numerous and more diverse than Medium or High Impact systems, NERC correctly chose to emphasize flexibility and responsiveness over imposing costly, rigid requirements. The NOPR's proposal to impose specific requirements could have the unintended consequence of reducing overall reliability by restricting that needed flexibility and responsiveness. In any event, there is no evidence that any purported improvement to reliability would justify the costs of mandating one-size-fits-all requirements on the various classes of Low Impact assets.

3. Alternatively, any directive on Low Impact cyber systems should ensure flexibility to redefine or subdivide the category

For the reasons described above, the Commission should accept, without modification, NERC's proposal for Low Impact cyber systems. But if the Commission nonetheless remains concerned that requiring responsible entities to implement documented cyber security policies will not properly reflect the risk of Low Impact assets, the Final Rule must allow NERC the flexibility to redefine or subdivide the Low Impact category.

The CIP v5 Standards, as proposed by NERC, leave no flexibility in determining which systems are categorized as Low Impact. But the proposed standards encourage responsiveness and adaptability by allowing flexibility in determining the methods for protecting those systems. If the Final Rule eliminates the flexibility of methods by directing NERC to develop and propose a revised standard that imposes specific cyber

controls on all Low Impact systems, the result would be a rigid, one-size-fits-all standard applied to a very broad and very diverse set of Low Impact cyber assets. Such an overbroad and unduly burdensome approach is likely to significantly increase costs, without significantly improving cyber security (and, as noted above, may even reduce reliability). The Commission could ameliorate that risk by allowing NERC to redefine or further subdivide the Low Impact category. Doing so would give NERC and the industry the opportunity to develop more tailored controls for the various classes of assets that would otherwise be lumped together in the Low Impact category.[6] Any directive on Low Impact systems must give NERC this flexibility so that NERC can develop an equally effective or superior solution to the Commission's concerns.

CONCLUSION

For the reasons set forth above, TAPS respectfully requests that the Commission approve, without modification, NERC's proposed CIP v5 Standards and the associated implementation plan. In particular, the Commission should not adopt the NOPR's proposed directive on Low Impact cyber systems. Alternatively, if the Final Rule nevertheless includes a directive on Low Impact cyber systems, TAPS requests that the Commission allow NERC the opportunity to redefine or subdivide the Low Impact category so that NERC can develop an equally effective or superior solution to the Commission's concerns.

---

[6] For example, the appropriate requirements for a microprocessor-based protective relay would have to be different from the requirements for a 1499 MW generator's control room.

Respectfully submitted,

/s/ Cynthia S. Bogorad

Cynthia S. Bogorad
Rebecca J. Baldwin
Latif M. Nurani

Attorneys for
Transmission Access Policy Study Group

Law Offices of:
Spiegel & McDiarmid LLP
1333 New Hampshire Avenue, NW
Washington, DC 20036
(202) 879-4000

June 24, 2013