UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Version 4 Critical Infrastructure Protection Reliability Standards	))	Docket No. RM11-11-000

COMMENTS OF SOUTHWEST POWER POOL REGIONAL ENTITY

On September 15, 2011, the Federal Energy Regulatory Commission ("FERC" or "Commission") issued a notice of proposed rulemaking ("NOPR") proposing to approve eight modified Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-4 through CIP-009-4, developed and submitted to the Commission for approval by the North American Electric Reliability Corporation (NERC), the Electric Reliability Organization certified by the Commission. Additionally, the Commission seeks comments from NERC and other interested persons regarding certain questions raised by the NOPR. Southwest Power Pool Regional Entity ("SPP RE") offers the following comments in response to the NOPR:

I. BACKGROUND

Southwest Power Pool, Inc. ("SPP") is a Commission-approved Regional Transmission Organization ("RTO"). It is an Arkansas non-profit corporation with its principle place of business in Little Rock, Arkansas. SPP is a transmission provider which administers transmission service to 64 Members, which include 14 investor-owned utilities, 11 municipal systems, 12 generation and transmission cooperatives, 4 state authorities, 7 independent power producers, 10 power marketers and 6 independent transmission company over portions of Arkansas, Kansas, Louisiana, Missouri, Nebraska, New Mexico, Oklahoma and Texas.

In addition to providing tariff services as an RTO, SPP serves as a Regional Entity ("RE") for NERC. SPP signed a Regional Entity Delegation Agreement with NERC and was

approved as an RE by the Commission on April 19, 2007[1]. In this capacity, SPP RE is responsible for enforcing NERC-approved reliability standards for all users, owners and operators of the bulk power system within the SPP RE footprint. SPP's RE-related activities are overseen by three independent Regional Entity Trustees. It is in its function as the Regional Entity that SPP makes these comments.

II. STATEGIES TO MEET OUTSTANDING ORDER 706 DIRECTIVES

The Commission identified three strategies that it believes NERC should consider to meet the outstanding directives from Order 706 and seeks comments on these strategies.[2] SPP RE believes Version 5 of the CIP Standards (CIP-002-5 through CIP-009-5 and CIP-010-1 through CIP-011-1 ("CIP V5 Standards")) partially address these strategies.

First, the Commission believes NERC should consider applicable features of the NIST Risk Management Framework to ensure protection of all cyber systems connected to the Bulk-Power System, including establishing CIP requirements based on entity functional characteristics rather than focusing on Critical Asset size. SPP RE believes the CIP V5 Standards have reasonably addressed this strategy. The CIP V5 Standards establish a NIST-like three-tiered classification of BES Cyber Systems based on potential impact, or risk, to the Bulk Electric System and made applicable to Responsible Entities based on their functional registration. Additionally, the system classification distinguishes between system types, including systems at a control center, systems with external routable connectivity, and access control and monitoring systems. Higher impacting BES and other cyber systems are subject to a greater number of increasingly stringent requirements, with some requirements applicable to all systems or Responsible Entities. The CIP V5 Standards have adopted bright line criteria to assign the impact rating, or tier, to a cyber system based upon the impact the functional obligations

---

1 *North American Electric Reliability Corp.*, 119 FERC ¶ 61,060, *order on reh'g*, 120 FERC ¶ 61,260 (2007).

2 *Version 4 Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, XX FERC Stats. & Regs., Proposed Regs. ¶ xx,xxx, 136 FERC ¶ 61,184 (2011) ("NOPR") at P 45.

performed and/or the span of control (e.g., MWs potentially impacted) of the cyber system. This is a marked change from the current CIP Standards, including the proposed Version 4 Standards, in that the preliminary step of identifying a Critical Asset has been eliminated. SPP RE agrees with this approach and believes that an outright adoption of the NIST guidelines (NIST SP 800-53 and other NIST special publications) is not appropriate to the electricity sector. The NIST guidelines are designed for a wide range of information systems and while certain aspects of SP 800-53 and SP 800-82 are applicable, the majority of the NIST framework does not appropriately address the unique circumstances of the electricity sector. Additionally, the NIST guidelines permit the agency to customize the security controls that the agency chooses to implement, which is contrary to the regulatory expectation of clearly defined, uniformly applied standards. The proper approach is to incorporate the NIST framework concepts into the sector-specific mandatory and enforceable standards, as the CIP V5 Standards have done.

Second, the Commission believes NERC should consider mechanisms for identifying Critical Cyber Assets by examining all possible communication paths between a given cyber resource and any asset supporting a reliability function. SPP RE believes that both the proposed CIP V4 and V5 Standards fail to consider this strategy. The proposed CIP V4 Standards define bright line criteria based upon the size of the asset in determining a Critical Asset and only then identify Critical Cyber Assets that support the reliable operation of the Critical Asset. As noted in the survey information provided by NERC and cited in the CIP V4 NOPR,[3] the CIP V4 bright line criteria is expected to leave 201 Control Centers (approximately 27 percent) out of scope to the CIP V4 Standards as a result of not meeting any of the control center criteria. The CIP V5 Standards rate BES Cyber Systems based upon their span of control and fail to consider the interconnectivity of the BES Cyber Systems and the potential for a small control center system to be used as a vector of attack against a larger control center system. Control center BES Cyber

[3] *Id.* at P 18.

Systems routinely exchange operational data with each other as required by NERC Reliability Standard TOP-005-2a.[4] This data is also provided to and between Reliability Coordinators in performance of the requirements of the Interconnection Reliability Operations and Coordination (IRO) Standards. The majority of operational data is exchanged electronically between BES Cyber Systems over wide area networks using the ICCP (TASE.2) protocol.

Third, the Commission believes NERC should provide a method for review and approval of Critical Cyber Asset lists from external sources such as the Regional Entities or NERC. Additionally, the Commission seeks comment whether the ERO and/or Regional Entities would have the ability, either in an event-driven investigation or compliance audit, to identify specific assets that fall outside the bright line criteria yet are still essential to Bulk-Power System reliability and should be subject prospectively to compliance with the CIP Reliability. If so, on what basis should that decision be made?[5]

The ERO and Regional Entities evaluate the Critical Cyber Asset lists today to determine if all of the Cyber Assets essential to the reliable operation of the Critical Asset have been properly identified as Critical Cyber Assets. SPP RE envisions performing similar analysis in the course of a compliance monitoring activity under the CIP V4 and V5 Standards. Under the CIP V5 Standards, SPP RE would shift from a subjective reliance upon the definition of a Critical Cyber Asset[6] to the application of the bright line criteria for BES and other Cyber System classification. SPP RE argues that it is not appropriate to arbitrarily apply criteria not found in the CIP Standards to require additional cyber systems to be subject to the CIP Standards. The correct approach would be the modification of the CIP Standards bright line criteria to address the deficiency.

---

4 *See* NERC Reliability Standards, TOP-005-2a (Requirement R2 requires Transmission Operators and Balancing Authorities to supply operating data to other Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability upon request).

5 NOPR at P 31.

6 *NERC Glossary*, Critical Cyber Asset definition.

Additionally, SPP RE encourages the Commission to require NERC to restore the "other" criteria to the bright line criteria. While it should be intuitively obvious to the Responsible Entities, the ERO, and the Regional Entities that the goal is to identify and protect all Critical Cyber Assets irrespective of the minimum set of Critical Assets derived by the bright line criteria, the absence of "other" could result in Responsible Entity reluctance to extend beyond that explicitly called for in the approved standard. Responsible Entities should be encouraged to consider local conditions in addition to the bright line criteria and include any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its Critical Asset list.

III. CONSIDERATION OF CONTROL CENTERS AS CRITICAL ASSETS

The Commission continues to express concern that "it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset."[7] The Commission noted that responsible entities should be required to "examine the impact on reliability if the control centers are unavailable, due for example to power or communications failures, or denial of service attacks" and to also "examine the impact that misuse of those control centers could have on the electric facilities they control and what the combined impact of those electric facilities could be on the reliability of the Bulk-Power System."[8]

SPP RE agrees with the Commission's concerns. The CIP V4 Standards continue to focus upon the potential impact of control centers upon the reliability of the Bulk Electric System without considering the interconnectivity of control centers and the possibility that a small network-connected control center deemed to not be a Critical Asset could be exploited, compromised, and used as a vector to attack and compromise the larger control center over the trusted networked communication paths. SPP RE believes that at a minimum, all Balancing

[7] NOPR at P 54.
[8] *Id.* at P 54.

Authority and Transmission Operator control centers should be unconditionally declared to be Critical Assets. SPP RE encourages FERC to consider requiring NERC to modify the bright line criteria to classify a control center as a Critical Asset, regardless of the entity's functional registration, if the control center is network-connected with one or more other control centers.

IV. CONSIDERATION OF COMMON CONTROL SYSTEMS AS CRITICAL ASSETS

Similar to the control center concerns, the Commission continues to express concern regarding the need to identify common control systems as Critical Cyber Assets, noting that "multiple assets, whether multiple generating units, multiple transmission breakers, or perhaps even multiple substations, could be taken out of service simultaneously due to a failure or misuse of the control system."[9] The Commission is concerned that even if one or all of the assets would not be considered as a Critical Asset on a standalone basis, a simultaneous outage resulting from the single point of control might affect the reliability or operability of the Bulk-Power System, stating "[i]n that case, the common control system should be considered a Critical Cyber Asset."[10]

SPP RE agrees with the Commission's concerns, noting for example that a number of wind farms manage relatively small generation units using a common control system. The individual generation resources do not qualify as Critical Assets, but in aggregate, from a common control perspective, pose reliability risks similar to properly identified Critical Assets. Regardless of whether the common control system is in a "control center" managing multiple sites or in a control room at a single plant or wind farm, the common control system should be identified as a Critical Cyber Asset. Under the CIP V4 Standards, the Responsible Entity would be expected to identify its "control center" or generation facility as a Critical Asset in order to bring the common control system into scope.

---

[9] *Id.* at P 55.

[10] *Id.* at P 55.

SPP RE is concerned that the bright line criteria fails to ensure all such common control systems are properly identified. Bright line criteria #1.1 will identify the single plant or wind farm that exceeds an aggregated net real power capability threshold of 1,500 MW as a Critical Asset, and should result in the identification of the common control system as a Critical Cyber Asset. Criteria #1.15 falls short in that it can be read to limit the controlled generation plants to those exceeding the 1,500 MW criteria specified in Criteria #1.1 when considering control centers as Critical Assets. It is not clear that Criteria #1.15 applies to control centers that control generation equal to or exceeding 1,500 MW in the aggregate regardless of plant size. Additionally, the term "control center" is not defined in the NERC Glossary or locally within CIP-002-4, resulting in potential disagreement as to what constitutes a "control center."

V. CIP V4 IMPLEMENTATION CONSIDERATION

SPP RE recommends the Commission consider allowing the Responsible Entities the option to "early adopt" the CIP V5 Standards once approved in lieu of continuing the overlapping effort necessary to comply with the CIP V4 Standards. Such early adoption would necessarily have to be an "all or nothing" cutover and would have to be formally declared by the Responsible Entity to its Regional Entity or Compliance Enforcement Authority. SPP RE suggests that the early adoption schedule would best apply to existing Critical Cyber Assets where the Cyber Assets are already compliant with the CIP Standards and work to conform to the revised CIP V5 Standard requirements should be less than that required for a newly identified Cyber System. SPP RE suggests that the BES Cyber Systems and other cyber systems that newly come into scope as a result of the CIP V5 Standards bright line criteria be afforded the full two year implementation schedule similar to the implementation schedule found in Table 3 of the current *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* posted on the NERC web site with the CIP Version 3 Standards.

VI. CONCLUSION

For the foregoing reasons, SPP RE respectfully requests that the Commission consider these comments and reflect SPP RE's recommendations in any final rule promulgated in this proceeding.

Stacy Dochoda
General Manager
Southwest Power Pool Regional Entity
16101 St. Vincent Way, Ste 103
Little Rock, AR 72223

November 18, 2011

Document Content(s)