UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure Protection Reliability Standards	**)** **)** **)** **)**	**Docket No. RM15-14-000**

COMMENTS OF THE ISO/RTO COUNCIL

The ISO/RTO Council (IRC)[1] respectfully submits these comments in response to the Federal Energy Regulatory Commission's (Commission) Notice of Proposed Rulemaking (NOPR) to approve critical infrastructure protection (CIP) Reliability Standards proposed by the North American Electric Reliability Corporation (NERC), and to direct NERC to develop requirements addressing supply chain management.[2]

I. COMMENTS

A. The IRC Appreciates the Commission's Focus on Addressing the Supply Chain Management Issues and asks that the Commission Address Certain Threshold Questions as to the Scope and Breadth of its Intended Efforts before Taking Further Action.

The IRC appreciates the Commission's discussion and concern regarding Information Technology (IT) supply chain management and the invitation to comment on, among other things, "the general proposal to direct that NERC develop a Reliability Standard to address supply chain management."[3] The IRC supports the Commission and Staff in their efforts to

[1] The IRC is comprised of the Alberta Electric System Operator (AESO), the California Independent System Operator Corporation (CAISO), the Electric Reliability Council of Texas, Inc. (ERCOT), the Independent Electricity System Operator (IESO), ISO New England Inc. (ISO-NE), the Midcontinent Independent System Operator, Inc. (MISO), the New York Independent System Operator, Inc. (NYISO), PJM Interconnection, L.L.C. (PJM) and the Southwest Power Pool, Inc. (SPP).

[2] *Revised Critical Infrastructure Protection Reliability Standards, Notice of Proposed Rulemaking*, 152 FERC ¶ 61,054, 80 Fed.Reg. 43354 (July 22, 2015) (*CIPS Rulemaking*).

[3] *CIPS Rulemaking* at P 42.

consider these very important issues and has identified four threshold issues that the Commission should address before it takes any further action in its attempts to mitigate risks associated with IT supply chain management, including directing NERC to address these issues through changes to a reliability standard. In particular, the IRC is concerned that the breadth and scope of the current directive is overly broad as proposed, which could hamper, not help, the achievement of the Commission's stated objective.

The threshold issues the Commission should consider before taking further action are:

1) the multi-faceted nature of the IT supply chain management issue and recognition of the need for coordination of this effort with other national and industry efforts underway;
2) the need for a focused and achievable scope of effort given the breadth of the issues and the many affected parties, including those outside the reach of the Commission's jurisdiction;
3) avoiding mandates on system operators that may expose them to compliance risk or liability associated with actions or omissions of third parties with little in the way of meaningful impact on upstream suppliers; and
4) the need for the Commission to develop a record to ensure a comprehensive assessment of the nature of the problem, the scope of remedies that are realistically achievable given the Commission's limited jurisdiction in this area, and the *pros* and *cons* of various potential paths forward.

The IRC's request is consistent with the Commission's directive to staff to "engage in additional outreach to further the Commission's consideration of the need for, and scope, content, and timing of a supply chain management standard," which recognizes the need for further dialogue and analysis in this area. This up-front scoping and information-gathering

effort, which the Commission should undertake through a technical conference in addition to staff-level outreach efforts, will provide critical information and clarification to and around the issues to be addressed. Moreover, such up-front scoping and discussion will pay significant dividends in terms of facilitating the implementation of any resulting, final directives.

As recognized by the Commission, the cybersecurity risk associated with the IT supply chain is embedded in the complex chains of global suppliers with varying degrees of practices and operations that impact products developed for industries that are vital to the U.S. economy, including the power sector. Unlike other reliability risks that are uniquely faced by the electric grid, IT supply chain risks are both more generic in scope and ubiquitous in nature, cutting across multiple vendors that supply services, underlying operating systems, commercial off-the-shelf software, and computer hardware that are not necessarily unique to the electricity sector. For example, a cybersecurity risk embedded in a state estimator application may well not be the result of any action or inaction of the vendor of the state estimator software, but, instead, result from risks and vulnerabilities in the underlying operating systems that are the foundation of the state estimator application.

As such, the risks of malware in such operating systems are faced not just by the electricity sector, but by all critical sectors of the economy that depend on those operating systems - ranging from the financial industry to the transportation industry and affecting countless industries in between. In the same vein, supply chain issues surrounding hardware such as servers, network devices, and firewalls are even broader in scope as such hardware is purchased and utilized by end users and business sectors throughout the U.S. and world.

The IRC members all have worked diligently to mitigate these risks using the tools available through their vendor procurement requirements in contracting for hardware and

software associated with bulk electric system operations. However, these efforts are varied and discrete, which does not allow suppliers or industries to benefit from the economies of scale. To this end, a well-focused set of requirements may provide benefits.

Before directing NERC (or any other entity) to launch a new sector-specific regulatory program, the IRC asks that FERC appropriately stage its efforts with the goal of developing a complete record that: 1) ensures that the scope of the effort is appropriate, and 2) the remedies adopted are feasible, practicable, and meaningfully advance the stated goal of enhancing cyber security over the long-term. Accordingly, the IRC proposes that the Commission and the industry utilize a risk-based process to further refine the scope of the directive. This process should acknowledge and leverage steps already underway both in the electric industry and other sectors of the economy. Further, it should evaluate the benefits and potentially adverse impacts of the use of Section 215 authority to address risks associated with IT supply chain management. The IRC supports a technical conference focused on the aforementioned threshold issues and up-front coordination both with system operators as well as with other government agencies (including those regulating other sectors critical to the economy such as financial services and transportation) as a key first step. The IRC also intends to participate in Commission-initiated outreach efforts and stands ready to work with the Commission on this important task.

B. Comments on Sufficiency of the Security Controls Regarding Bulk Electric System Communication Networks

The Commission seeks comments on proposals pertaining to security controls for Bulk Electric System (BES) communication networks. Pursuant to section 215(d)(5) of the Federal Power Act, the Commission proposes to direct NERC to develop a modification to proposed Reliability Standard CIP-006-6 to require responsible entities to implement controls to protect, at

a minimum, all communication links and sensitive BES data communicated between all BES Control Centers.

The IRC agrees that inter-Control Center communications play a vital role in maintaining BES reliability and that timely and accurate communication between Control Centers is important for maintaining situational awareness and the reliable operation of the BES. While the IRC supports further evaluation of additional cybersecurity protections for inter-Control Center communications and the creation of standard revisions, if deemed necessary, the IRC requests that the Commission consider only the activities and controls that are within the purview, authority, and capability of the responsible entity as they consider the need for additional action and protections. Additionally, to ensure consistency with the risk-based foundation already established in the CIP reliability standards, the IRC requests that new requirements consider the potential impact of particular Control Centers on reliability, *e.g.*, High, Medium, Low, and that any new requirements be result-based and not overly prescriptive. This approach is necessary to allow the responsible entities sufficient flexibility in the implementation and tailoring of technologies and mitigating controls that may already exist. This strategy will also provide that any additional, required protections are customizable to the particular network configuration and hardware and software characteristics that responsible entities have already implemented. Where protections are not flexible, implementation of particular protections in certain configurations and systems could actually diminish the cybersecurity protections that are already established, which result would be contrary to the stated objective to enhance the cybersecurity protection of the BES.

C. Comments on Protections during Interactive Remote Access

The Commission requests comments on the value achieved if the CIP standards were to require the incorporation of additional network segmentation controls, connection monitoring, and session termination controls behind responsible entity intermediate systems. In particular, the Commission asks whether these or other steps to improve remote access protection are necessary and whether the adoption of any additional security controls addressing this topic would provide substantial reliability and security benefits.

The IRC notes that the CIP Version 5 requirements addressing Interactive Remote Access (CIP-005-5, R2) have not been fully implemented or reached their effective enforcement date. Without full implementation, it is difficult to identify any gaps or the need for any additional protections. The Commission-approved CIP v5 Reliability Standards at CIP-003-6, CIP-004-6, CIP-005-5, and CIP-007-6 require responsible entities to implement a number of security controls for electronic access, including the Intermediate Systems meeting the criteria of Electronic Access Control and Monitoring Systems. These substantial additional protections should be implemented fully in the near future. The IRC, therefore, requests that responsible entities be given the time allotted to implement the currently-approved requirements and associated protections, and to gain experience with such controls before the Commission requires additional protections. This approach will allow the Commission, NERC, Regional Entities, and responsible entities the opportunity to evaluate the effectiveness of newly implemented access-related controls, which experience and evaluation will help to inform, determine, and appropriately address any remaining potential gaps, risks, or other needs.

II. CONCLUSION

WHEREFORE, the IRC respectfully asks that the Commission accept the IRC's comments and grant the IRC's requests as specified herein.

Respectfully submitted,

/s/ Anna A. McKenna
Roger E. Collanton,
General Counsel
Anna A. McKenna*
Assistant General Counsel
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ Carl F. Patka
Robert E. Fernandez, General Counsel
Raymond Stalter
Director of Regulatory Affairs
Carl F. Patka*
Assistant General Counsel
Christopher Sharp
Compliance Attorney
New York Independent System Operator, Inc.
10 Krey Boulevard
skeegan@nyiso.com

/s/ Theodore J. Paradise
Raymond W. Hepper
Vice President, General Counsel, & Secretary
Theodore J. Paradise*
Assistant General Counsel, Operations and Planning
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
tparadise@iso-ne.com

/s/ Craig Glazer
Craig Glazer*
Vice President - Federal Government Policy
Robert V. Eckenrod*
Senior Counsel
PJM Interconnection, L.L.C.
Suite 600
1200 G Street, N.W.
Washington, D.C. 20005
202-423-4743
Craig.Glazer@pjm.com
Robert.Eckenrod@pjm.com

/s/ Diana Pommen
Diana Pommen,* Director Interjurisdictional Affairs and Compliance
Alberta Electric System Operator
2500, 330 – 5 Avenue SW
Calgary, Alberta T2P 0L4
diana.pommen@aeso.ca

/s/ Jessica Savage
Jessica Savage,* Manager, Government and Regulatory Affairs
Independent Electricity System Operator
655 Bay Street, Suite 410
Toronto, ON M5G 2K4
Jessica. savage@ieso.ca

/s/ Stephen G. Kozey
Stephen G. Kozey*
Vice President, General Counsel, and Secretary
Erin M. Murphy*
Managing Assistant General Counsel
Midcontinent Independent System Operator, Inc.
P.O. Box 4202
Carmel, Indiana 46082-4202
skozey@midwestiso.org

/s/ Paul Suskie
Paul Suskie
Sr. VP Regulatory Policy
& General Counsel
Matt Morais,*
Associate General Counsel - Markets and Regulatory Policy.
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

/s/ Christina V. Bigelow
Christina V. Bigelow*
Lead Corporate Counsel, Federal Policy
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
Christina.bigelow@ercot.com

/s/ Nancy Marconi
Nancy Marconi, Manager, Regulatory Affairs
Independent Electricity System Operator
1600-120 Adelaide Street, West
Toronto, Ontario M5H1T1
Nancy.Marconi@ieso.ca

**Designated to receive service*

Dated: September 21, 2015

CERTIFICATE OF SERVICE

I hereby certify that I have served the foregoing document upon the parties listed on the official service lists in the above-referenced proceedings, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated at Folsom, California this 21st day of September 2015.

/s/ Anna Pascuzzo

Anna Pascuzzo