UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure	**)**	
Protection Reliability Standards	**)**	
Notice of Proposed Rulemaking	**)**	**Docket No. RM15-14-000**

COMMENTS OF THE MIDCONTINENT INDEPENDENT SYSTEM OPERATOR, INC.

I. Introduction

Midcontinent Independent System Operator, Inc. (MISO) appreciates the Commission's concern regarding the issues and risks impacting the Information Technology (IT) Supply Chain Security Management (SCSM) on the Bulk Electric System (BES); and welcomes the invitation to comment and present to the Commission on this topic.

John Goode, MISO's Senior Vice President and Chief Information Officer (CIO) is responsible for our IT strategy, execution, and operations. Mr. Goode is representing MISO and will be presenting our comments concerning this topic.

Prior to MISO, Mr. Goode served as the CIO of the Boston Options Exchange; head of technology for Swiss Bank Corporation's global foreign exchange business; VP of electronic trading systems at the Chicago Mercantile Exchange; and was the global head of e-business technology and VP of Technology Architecture for Baxter International. With these various industries, Mr. Goode has been widely exposed to the regulatory impacts as it pertains to Cyber Security and supply chain management.

II. Summary Overview of Comments

Our comments can be summarized in four basic points:

1. MISO supports supply chain security management guidance or standards for the electric industry and the reliability and security of the BES. In order to sustain the necessary security and reliability, MISO supplements compliance with the CIP Standards through our defense-in-depth and intelligence-driven methodologies;
2. In order to get supply chain security management program in place quickly that is effective, the industry should use prior, proven frameworks for supply chain security such as those in the financial industry;
3. These security frameworks should be risk-based reviews of controls that are then verified and attested to by an independent third-party similar to those reviews performed in the financial industry; and
4. Direction on supply chain security management should be in the form of a mandatory guidance document for the electric industry so that we can gauge the application and effectiveness of the guidance, third-party reviews and attestations, before the industry expends significant time and money in the development of a stand-alone CIP standard that may be a challenge to enforce against supply chain vendors.

III. Background

MISO, as a Regional Transmission Organization (RTO), is in a unique class within its relationship with the BES. We see MISO's role as providing technology based solutions and services to ensure BES reliability versus directly controlling the BES for the electric industry. As a technology solutions provider for this industry, our supply chain is extensive and includes

some of the largest technology vendors in the world (e.g. CISCO, IBM, & HP). As an RTO, MISO has taken an enterprise risk management approach to managing our business, technology assets, and supply chain.

IV. MISO's SCSM Program Approach

MISO views compliance to specific CIP Standards as the minimum required and, therefore, we are continually seeking to embrace additional security standards and best practices beyond those just required for CIP compliance. The MISO SCSM program leverages the use of practices proven to be effective in the financial industry to assess the criticality of the functions performed by our supply chain vendors, as well as their Cyber Security capability maturity, and then apply oversight and control based upon the outcome of those assessments. We actively engage with our most critical supply chain vendors through site visits and routine service level reviews, to ensure that issues and challenges are quickly identified and resolved. We are also taking measures to more explicitly articulate Cyber Security expectations in contract language to further ensure that security risks are addressed.

The above approach for the MISO SCSM works in the context of an overall MISO Cyber Security Strategy approved by Executive Senior Management and the MISO Board of Directors which takes a defense in depth and intelligence driven security approach to managing Cyber Security risks.

V. Current CIP Standards Coverage of SCSM for the BES Industry

The current CIP Standards address the obligations of Registered Entities, which are subject to Commission jurisdiction, such as MISO. However these Standards do not directly

impose obligations on industry supply chain vendors, suppliers, and other entities that provide products and services to the industry. Due to jurisdiction, the mitigation of this risk is placed on the Registered Entity who leverages contractual negotiations for audit provisions which may not effectively minimize security risks to the BES. Additionally, the current CIP Standards do not address the upstream development and delivery processes of critical system designs and modifications that could build in proactive security measures prior to use by a Registered Entity.

As such, with any CIP Standard, current or future, MISO will continue to supplement with standards and best practices beyond those just required for CIP compliance to ensure we maintain comprehensive Cyber Security and SCSM programs.

VI. The Usefulness of Standards - A Welcoming Approach

MISO welcomes and supports changes to standards and regulations that foster consistency in approach throughout the industry, while allowing for variations in approach. This can ensure our unique relationship with the BES that provides technology solutions can be effectively managed and improved over time as it relates to Cyber Security.

VII. MISO Recommendations

MISO recommends that FERC adopt the use of standalone technical guidance or a new CIP Standard that directly adopts standards and best practice frameworks already employed by many of the largest technology providers. Adoption of this strategy will accelerate efforts to address the risks related to Cyber Security and SCSM in our industry. We are concerned that a discrete CIP Standard for SCSM written solely for the electric industry would not be as effective as leveraging existing proven standards/practices. We also believe the creation and effective

implementation of a discrete SCSM CIP standard will have a longer adoption cycle. A discrete SCSM CIP Standard would involve extended stakeholder debate, regulatory review processes, additional costs, and added compliance complexity to suppliers already struggling to integrate a myriad of separate regulations driven from different industry perspectives.

VIII. Reuse of Existing Standards

There are a number of existing standards and best practice frameworks in use by other industries that are proven and that have the potential for reuse upon further investigation. The sheer number of existing standards and frameworks illustrates and reinforces MISO's recommendation that FERC should adopt a framework already in use. First, it illustrates that if the electric industry creates another discrete SCSM CIP Standard, that standard will be added to a long list of separate and distinct standards technology vendors are already having difficulty integrating and implementing for compliance. Second, it suggests what the electric industry is seeking to do with SCSM has already been done by industries that are more advanced and mature in Cyber Security. Therefore, the electric industry has the unique opportunity to accelerate its efforts by simply adopting an existing approach in lieu of creating another set of separate requirements via a new discrete SCSM CIP Standard.

Potential Standards and Frameworks for adoption are:

- National Institute of Standards and Technology (NIST) offers several solutions. NIST 800-161 for Supply Chain Risk Management Practices and NIST 800-53R4 for Security and Privacy Controls are utilized by the federal government and the big four accounting firms. The NIST standards bring together several well-known frameworks and provide coverage across diverse business scenarios;

- The Federal Risk and Authorization Management Program is an existing government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This program allows for the independent assessment by accredited Third Party Assessment Organizations.
- Securities and Exchange Commission Regulation on Systems Compliance and Integrity to monitor the security and capabilities of the U.S. securities markets' technological infrastructure;
- AICPA (American Institute of CPAs) Service Organization Controls (SOC) process is designed to help service organizations, organizations that operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant. Reporting and Attesting to controls outlined in SOC 1, SOC 2, & SOC 3, is a model that is already extensively used in the industry that could be a model for FERC.
- The HITRUST CSF is a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management. Developed in collaboration with healthcare and information security professionals, the HITRUST CSF rationalizes healthcare-relevant regulations and standards into a single overarching security framework. Certification is done by qualified third party assessors.
- The Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook, that includes Appendix J: "Strengthening the

Resilience of Outsourced Technology Services" Focuses on third-party technology service providers that perform or support critical operations in a secure and recoverable manner, and covers Third-Party Management, Third-Party Capacity, Testing with Third-Party and Cyber Resilience.

- The Payment Card Industry Data Security Standard (PCI DSS) is designed to ensure the safe handling of cardholder information at every step of payment card processing through effective use of specifications, tools, measurements, and support resources, to include security of third-parties and provides for a means to leverage qualified third parties to assess and qualify against this Standard.
- Shared Assessment framework utilized by the big four accounting firms to assess supply change risk consistently across the financial industry.

Leveraging approaches similar to those listed above would benefit the electric industry. First, it addresses some of the issues with the limited jurisdictional reach that the Commission and NERC have on industry supply chain vendors and also allows the electric industry to leverage years of effort and toil of industries to address similar risks with SCSM. In addition, it offers the opportunity for the electric industry, struggling like other industries to recruit security talent, to leverage the expertise of third-party security assessors. The output from third-party assessments could then be supplied to all of the vendors' customers providing multiple benefits including but not limited to, enhanced quality improvements and reduced time and cost for each Registered Entity and each vendor participating in regulatory and operations audits. A periodic review of the Registered Entities supply chain vendor management process could be leveraged over time for further assurances to FERC.

IX. Managing Diverse Group of Vendors Requires a Risk-Based Standards Approach

MISO, like other registered entities, works with both enterprise-business class vendors such as CISCO, HP, AT&T, Microsoft, and Red Hat, as well as electric industry-specific vendors such as Alstom and OATI. Enterprise-business class vendors tend to provide exceptional service and follow well-vetted industry standards and best practices. However, these types of companies do not typically allow their customers to directly assess their processes. They will, however, frequently provide a level of attestation to the certifications they follow. For example, companies listed in the International Standard Organization certification registry certify to following a specific set of standards/guidelines and affirm that certain certifications have been obtained.

Large IT enterprise-business class vendors have already been required to advance their Cyber Security capabilities and assure the industries they serve of their security and compliance posture, as they were asked much earlier than the electric industry for those assurances. For example, companies like CISCO, Microsoft, HP, Oracle, and others were early adopters of control frameworks because their business model required it much sooner than the electric industry.

We believe those in the electric industry that leverage supply chain vendors that strictly serve or focus solutions on the electric industry are in greater need of SCSM improvements simply due to the electric industry relatively less mature state of security. Common electric industry-specific vendors, that provide modifications to our critical systems used to manage the BES, employ a less consistent and sophisticated use of development best practice approaches and quality in their processes and procedures for the modification of these critical systems. The potential impact of defects introduced by vendors is higher in critical systems directly impacting

the electric grid versus vendors used for less critical systems. Electric industry-specific vendors, when asked for greater security practice assurance and attestation, have often also cited higher costs with limited return.

The electric industry, dependent upon a very few vendors in this space, has historically lacked the motivation to change in response to ad hoc requests. Without a more standardized approach provided by the industry, the desired improvements from our supply chain vendors would place larger risk and cost on Registered Entities. MISO also believes extending the reach of NERC Standards to supply chain vendors will require an adjustment to the auditing approach to ensure Registered Entities can demonstrate compliance. Due to the sensitivity of security information and evidence, it is unlikely vendors would be willing to provide such documentation, therefore, Registered Entities will not have access to the specific system and security information of their supply chain vendors to provide as evidence.

MISO recommends a risk-based approach to evidence and auditing be applied to whatever guidance or standards approach is ultimately embraced, due to the varying levels of maturity demonstrated between enterprise-class vendors and the electric industry-specific vendors.

X. Overall MISO Recommendations:

FERC should direct that a pilot be initiated as an expedient first step and then direct the industry to develop a mandatory guidance document that outlines for the electric industry existing standards and best practice frameworks that may be leveraged to address SCSM. Lessons learned from this pilot should then be used to refine the mandatory guidance document to inform how best to move forward with a SCSM CIP Standard that allows for adoption and

use of existing standards and best practice frameworks. Any guidance or Standard should offer a means for risk-based auditing and evidence review of the Registered Entities supply chain.

XI. COMMUNICATIONS

All correspondence and communications in this matter should be addressed to:

Mark Brooks, Executive Director &
Chief Information Security Officer
Midcontinent Independent
System Operator, Inc.
P.O. Box 4202
Carmel, IN 46082
(317) 249-5400 (telephone)
(317) 249-5912 (facsimile)
mbrooks@misoenergy.org

Jacob Phillips, Senior Corporate Counsel
Midcontinent Independent
System Operator, Inc.
P.O. Box 4202
Carmel, IN 46082
(317) 249-5400 (telephone)
(317) 249-5912 (facsimile)
jrphillips@misoenergy.org

Kimberle Seale, Executive Director
IT Strategy & Business Operations
Midcontinent Independent
System Operator, Inc.
P.O. Box 4202
Carmel, IN 46082
(317) 249-5400 (telephone)
(317) 249-5912 (facsimile)
kseale@misoenergy.org

XII. Conclusion:

MISO thanks the Commission for this opportunity to provide our remarks. We support the Commission's attention on the supply chain management issues and risks we face and encourage the Commission actions to help the electric industry. We recommend that FERC adopt the use of standalone technical guidance or a new CIP Standard that directly adopts

standards and best practice frameworks already in use today by many of the largest technology providers to accelerate efforts to address the risks related to Cyber Security and SCSM in our industry.

Respectfully submitted,
/s/ John Goode
John Goode
Midcontinent Independent
System Operator, Inc.
P.O. Box 4202
Carmel, Indiana 46082
Telephone (317) 249-5400
Facsimile (317) 249-5912

Chief Information Officer for the
Midcontinent Independent System Operator,
Inc.

Dated: January 15, 2016