167 FERC ¶ 61,229
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Neil Chatterjee, Chairman;
Cheryl A. LaFleur, Richard Glick,
and Bernard L. McNamee.

Midcontinent Independent System Operator, Inc. Docket Nos. ER19-875-000
ER19-875-001

ORDER ON PROPOSED TARIFF REVISIONS

(Issued June 20, 2019)

1. On January 28, 2019 (January 28 Filing), as amended on April 22, 2019, Midcontinent Independent System Operator, Inc. (MISO) filed, pursuant to section 205 of the Federal Power Act (FPA),[1] proposed modifications to its Open Access Transmission, Energy, and Operating Reserve Markets Tariff (Tariff). MISO explains that the proposed modifications will (1) allow for the sharing of non-public information with federal agencies that have cybersecurity responsibilities, (2) reconcile the aforementioned adjustments with existing Tariff provisions, and (3) make non-substantive adjustments to increase readability. As discussed below, we accept MISO's proposed Tariff revisions, effective March 30, 2019, as requested.

I. Background

A. Existing Federal Information Sharing Requirements

2. On March 28, 2013, the Commodity Futures Trading Commission (CFTC) issued an order[2] granting certain independent system operators (ISO) and regional transmission

[1] 16 U.S.C. § 824d (2012).

[2] *Final Order in Response to a Petition From Certain Independent System Operators and Regional Transmission Organizations to Exempt Specified Transactions Authorized by a Tariff or Protocol Approved by the Federal Energy Regulatory Commission or the Public Utility Commission of Texas From Certain Provisions of the Commodity Exchange Act Pursuant to the Authority Provided in the Act*, 78 Fed. Reg. 19,880 (April 2, 2013) (CFTC Final Order).

(continued ...)

organizations (RTO) exemptions from the CFTC regulations under the Dodd-Frank Wall Street Reform and Consumer Protection Act.[3] The CFTC Final Order contained certain conditions that the ISOs/RTOs had to meet in order to be eligible for the exemption, including, among other things, that their tariffs authorize the sharing of market data and information with the CFTC without notice to market participants. To satisfy these conditions, MISO, in Docket No. ER13-1895-000, amended Section 38.9.3 of its Tariff to provide the same treatment to information requests from the CFTC or its staff that MISO provided to requests from the Commission at that time. Under this treatment, MISO would only notify an entity that it shared the entity's confidential information with the Commission or the CFTC if the agency specifically requested that MISO provide notification. The Commission accepted MISO's Tariff changes on September 3, 2013.[4]

B. Executive Orders on Cybersecurity

3. In recent years, cybersecurity concerns have led to the issuance of several Presidential Executive Orders (Executive Orders). Presidential Executive Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, issued on February 19, 2013, sought to enhance security and resiliency of critical infrastructure through voluntary, collaborative efforts involving federal agencies and owners/operators of privately-owned critical infrastructure, such as MISO.[5] Additionally, Presidential Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* issued on May 19, 2017, directed the Department of Homeland Security (Homeland Security), in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation (FBI), and heads of various agencies, to, among other things, identify authorities and capabilities that agencies could employ to support cybersecurity efforts of certain entities, such as MISO.[6]

[3] Pub. L. No. 111-203, 124 Stat. 1376 (2010).

[4] *Midcontinent Indep. Sys. Operator, Inc.*, 144 FERC ¶ 61,177, at PP 2-3 (2013).

[5] January 28 Filing, Transmittal at 2 (citing Executive Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11,739 (February 19, 2013)).

[6] *Id*. (citing Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22,391 (May 16, 2017)).

(continued ...)

C. Ongoing Commission Directives for Cybersecurity Information Sharing

4. In Order No. 848,[7] pursuant to section 215(d)(5) of the FPA, the Commission directed the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), to develop and submit modifications to the Critical Infrastructure Protection (CIP) Reliability Standards[8] to improve the reporting of cybersecurity incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system. The Commission noted that the development of modified mandatory reporting requirements would improve awareness of existing and future cybersecurity threats and potential vulnerabilities.[9] The Commission directed NERC to develop and submit modifications to the CIP Reliability Standards to require the reporting of cybersecurity incidents that compromise, or attempt to compromise, a responsible entity's electronic security perimeter or associated electronic access control or monitoring systems. The Commission observed that cybersecurity incidents are presently reported by responsible entities in accordance with Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning). However, under Reliability Standard CIP-008-5, responsible entities must only report cybersecurity incidents if they have compromised or disrupted one or more reliability tasks. The Commission explained that the current reporting threshold may understate the true scope of cyber-related threats facing the Bulk-Power System, particularly given the lack of any reportable incidents in 2015 and 2016.[10]

[7] *Cyber Security Incident Reporting Reliability Standards*, Order No. 848, 164 FERC ¶ 61,033 (2018).

[8] Section 215(a)(3) of the FPA defines Reliability Standard as: "a requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the bulk-power system, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity." 16 U.S.C. § 824o(a)(3) (2012).

[9] Order No. 848, 164 FERC ¶ 61,033 at PP 2, 66.

[10] *Id.* PP 2, 9.

(continued ...)

5. In response, on March 7, 2019, in Docket No. RD19-3-000, NERC submitted a petition for approval of proposed Reliability Standard CIP-008-6, which the Commission is granting in an order being issued contemporaneously with this order.[11]

II. MISO's Proposed Tariff Revisions

6. MISO states that the instant filing stems from stakeholder discussions initiated in response to concerns about the increasing threat of cybersecurity attacks on the reliable operation of its transmission system. MISO states that it also participated in federal initiatives in response to the Executive Orders to help identify information that would be appropriate to share during a cybersecurity incident and the terms and conditions for sharing that information with Homeland Security.[12]

7. MISO proposes modifications to its Tariff to enhance its ability to coordinate with federal agencies in cybersecurity emergencies. MISO proposes to amend portions of Section 38.9.1 through 38.9.3(A) in Module C of its Tariff in order to: (1) permit the sharing of non-public information with federal agencies that have cybersecurity responsibilities, (2) reconcile the aforementioned adjustments with existing Tariff provisions, and (3) make non-substantive adjustments to increase readability. MISO also proposes to define a new term in Module A of its Tariff.

8. Specifically, MISO proposes to amend portions of Section 38.9 (Confidentiality), which pertains to MISO's protection and controlled release of non-public information. MISO explains that existing Section 38.9.3 already permits the sharing of confidential information with the Commission and the CFTC or their staff. While retaining the Commission's and the CFTC's ability to request and receive non-public information, MISO proposes to reorganize Section 38.9.3 to authorize MISO to provide information to other federal agencies and organizations in response to a "Cyber Exigency;" MISO also proposes to define Cyber Exigency in Module A of its Tariff.[13] MISO proposes to generalize the language in Section 38.9.3 to refer to federal agencies and organizations, which MISO argues is consistent with proposed Reliability Standard CIP-008-6 that will

[11] *North American Electric Reliability Corporation*, 167 FERC ¶ 61,230 (2019).

[12] January 28 Filing, Transmittal at 4, 7-8.

[13] MISO proposes to define Cyber Exigency as: "A suspicious electronic act or event that has the potential to compromise reliability within the Transmission Provider Region or other electrical facilities directly or indirectly connected to the Transmission System and whose severity reasonably requires that the Transmission Provider obtain expert assistance not normally called upon to counter such an electronic act or to resolve such an event." January 28 Filing, Proposed Tariff, Module A, Section 1 (Definitions).

(continued ...)

authorize MISO to share cybersecurity information with NERC and NERC's Regional Entities. MISO explains that the proposed relationship would authorize voluntary data sharing by MISO with federal cybersecurity authorities under extreme cybersecurity conditions to facilitate government-industry cooperation as contemplated by the Executive Orders[14] without imposing unduly burdensome and unnecessary requirements upon MISO to release information that is not normally released.

9. Within Section 38.9.3.a (Specified Agencies/Organizations and Treatment of Confidential Information), MISO proposes to designate the existing provision for sharing information with the Commission and the CFTC as Section 38.9.3.a.i. Similarly, MISO proposes to insert a parallel provision as Section 38.9.3.a.ii to permit MISO to share information in response to a Cyber Exigency with any federal agency with cybersecurity responsibilities, such as Homeland Security or the FBI. MISO explains that the proposed expansion to include additional federal agencies is limited, as information sharing will occur only in situations that involve a Cyber Exigency. MISO also states that it will be under no obligation to provide information to additional federal agencies, although it may seek help under severe circumstances.[15] MISO states that it does not intend to share information with any federal agency without prior mutual agreement regarding the terms under which data sharing would occur and that any data sharing would be limited.[16]

10. Additionally, MISO proposes, in Section 38.9.3.a.iii, to permit data sharing with NERC and NERC's Regional Entities if MISO determines that the information sharing will enhance or maintain reliability. MISO proposes to move a provision for data sharing with NERC and NERC's Regional Entities from current Section 38.9.1 to Section 38.9.3.a.iii.[17] MISO states that the proposal harmonizes the treatment of sharing information with NERC and NERC's Regional Entities with its treatment of the Commission and the CFTC in Section 38.9.3 of the Tariff, which does not require notification to an affected market participant in advance of sharing information.[18]

---

[14] January 28 Filing, Transmittal at 1-2, 4, 8.

[15] *Id.* at 5.

[16] *Id.* at 7.

[17] MISO explains that section 38.9.1 contains broad overview provisions regarding confidentiality requirements, and as such, MISO believes this section is less suited for discussing specific exceptions to information sharing limitations compared to Section 38.9.3. *Id.* at 5-6.

[18] *Id.*

(continued ...)

11. MISO states that the additional revisions to Section 38.9.3 reconcile the proposed adjustments with existing Tariff provisions. In new Section 38.9.3.b (Request for Confidential Data), MISO proposes to expand the existing provision in Section 38.9.3, that requires the Commission and the CFTC to treat any shared information as confidential and non-public, to any federal agency or organization covered in proposed Section 38.9.3.a.[19] For example, MISO proposes to replace references to governing regulations for information sharing with the Commission and the CFTC with "Applicable Laws and Regulations."[20] Similarly, in new Section 38.9.3.c (General Provision for Release of Information to Third Parties), MISO proposes to generalize a provision regarding the notification of market participants, that currently applies when MISO receives a request by the Commission or the CFTC to share information with third parties, to apply to a request by a federal agency or organization covered under proposed Section 38.9.3.a. MISO explains that it will notify market participants by appropriate means based on the individual circumstances of each situation (e.g., time requirements, breadth of persons affected, and information requested).[21]

12. In terms of non-substantive adjustments, MISO proposes to reposition Section 38.9.3(A) (Electronic Delivery of Confidential and Non-Public Data to the Commission) to Section 38.9.3.d; add titles and other adjustments to Sections 38.9.1, 38.9.2, and 38.9.3 for unified appearance; and make other ministerial adjustments to increase readability, such as changing "confidential data or information" to the defined term "Confidential Information."[22]

13. MISO states that it discussed the proposed modifications with stakeholders at its Reliability Subcommittee meeting on November 1, 2018, posted the redlined Tariff sheets for stakeholder review, solicited stakeholder comments on the proposed modifications, and responded to those comments at a follow-up Reliability Subcommittee meeting on November 29, 2018. MISO claims that it received two written comments from stakeholders in November 2018 reflecting comfort with the proposed revisions, as

[19] *Id*. at 6.

[20] MISO defines "Applicable Laws and Regulations" as: "All duly promulgated applicable federal, state and local laws, regulations, rules, ordinances, codes, decrees, judgments, directives, or judicial or administrative orders, permits and other duly authorized actions of any Governmental Authority having jurisdiction over the Parties, their respective facilities and/or the respective services they provide." January 28 Filing, Proposed Tariff, Module A, Section 1 (Definitions).

[21] January 28 Filing, Transmittal at 6.

[22] *Id*. at 6-7.

(continued ...)

well as written inquiries from another stakeholder in January 2019 reflecting the issues raised during the stakeholder meeting.[23]

14. MISO requests an effective date of March 30, 2019 for its proposed Tariff revisions.

15. On March 22, 2019, Commission staff issued a deficiency letter (Deficiency Letter) to which MISO responded on April 22, 2019 (Deficiency Response).

A. Notice of Filings and Responsive Pleadings

16. Notice of MISO's January 28, 2019 filing was published in the *Federal Register*, 84 Fed. Reg. 1721 (2019), with interventions and protests due on or before February 19, 2019. Exelon Corporation (Exelon), American Municipal Power Inc., Consumers Energy Company, Ameren Services Company, International Transmission Company, Energy Services LLC, and Public Citizen Inc. filed timely motions to intervene. On March 5, 2019, Exelon filed a motion for leave to file comments out of time and comments. On March 18, 2019, MISO filed an answer.

17. Notice of the Deficiency Response was published in the *Federal Register*, 84 Fed. Reg. 17,823 (2019), with interventions and protests due on or before May 13, 2019. None was filed.

1. Exelon's Comments

18. Exelon requests that the Commission accept its motion to file comments out of time, given the importance of the subject matter to the reliability of the electric grid and its need to delve into various laws to ensure that the proposed Tariff changes protect confidential information. Exelon emphasizes that the Commission may allow a response out of time where there is no showing of any undue prejudice or delay.[24]

19. Exelon alleges that MISO's proposed Tariff revisions fail to adequately protect confidential information.[25] Exelon contends that the proposed Tariff revisions would not restrict the federal agencies to which confidential information may be disclosed, the circumstances under which such information may be disclosed, and the manner in which

[23] *Id*. at 7-8.

[24] Exelon Comments at 1-2.

[25] *Id.* at n.1 (citing *Trans Alaska Pipeline System*, 104 FERC ¶ 61,201, at P 6 (2003); *Natural Gas Pipeline Company of America*, 66 FERC ¶ 61,310 (1994)).

(continued ...)

such information may be disclosed. Exelon requests that the Commission reject MISO's filing without prejudice to MISO filing another proposal that addresses Exelon's concerns.[26]

20. First, Exelon argues that MISO should modify its proposal to narrow the federal agencies to which MISO may disclose information.[27] Exelon contends that disclosures should be limited to federal agencies possessing cybersecurity responsibility for the energy sector, as established by the FPA and the Critical Infrastructure Information Act of 2002,[28] and to federal agencies responsible for cyber threat indicators and defensive measures under the Cybersecurity Information Sharing Act of 2015.[29]

21. Second, Exelon requests that MISO modify its proposal to narrow the type of situations where information may be disclosed. Exelon believes that because the proposed disclosure provision in Section 38.9.3.a is too broad, it would be difficult to claim that any information sharing was inappropriate. Exelon argues that the definition of Cyber Exigency should be limited to emergency-type situations where coordination of information disclosure with asset owners would be impractical.[30]

22. Third, Exelon requests that MISO modify its proposal to enhance information protection requirements by referencing in the Tariff the statutory regimes under which the information would be shared. For example, Exelon explains that proposed Section 38.9.3.a.ii does not limit interagency sharing to circumstances in which the other agencies must follow Freedom of Information Act (FOIA)[31] exemption rules, and that proposed Section 38.9.3.b only requires MISO to "request" confidential and non-public treatment. Exelon also contends that the proposed changes weaken information sharing protections with the Commission and the CFTC by eliminating references to the

[26] *Id.* at 1-2.

[27] *Id.* at 3.

[28] 6 U.S.C. § 131.

[29] P.L. 114-113, Division N, Title I, 129 Stat. 2936 (2015).

[30] Exelon Comments at 3.

[31] 5 U.S.C. § 552 (2012).

(continued ...)

regulations mandating protections for information shared, and Exelon prefers that those references remain in the Tariff.[32]

23. Fourth, Exelon requests that MISO enhance notification provisions by requiring MISO to notify an entity prior to, or at least as soon as practicable, following information release to a federal agency. Exelon contends that under proposed Section 38.9.3.c, MISO's only obligation to notify an entity that MISO has passed the entity's information to a federal agency is if the federal agency asks to disclose that information to a third party that is not a federal agency. Exelon believes that the proposed language significantly reduces MISO's obligations to notify an entity if MISO discloses or plans to disclose the entity's confidential information because, under the current Tariff, a generator would be notified of any federal agency requests for information.[33]

24. Fifth, Exelon requests that MISO establish internal procedures in advance of any incident to ensure the maximum protection of confidential information. Exelon argues that MISO will not have the opportunity to identify the applicable laws in an emergency and that, therefore, MISO should develop an internal "playbook" in advance, with clear instructions based on the type of information to be released, detailing the requirements and responsibilities related to the release of information.[34]

2. MISO's Answer

25. MISO requests that the Commission deny Exelon's motion to file comments out of time, arguing that Exelon failed to provide a credible justification for its untimely comments, which MISO characterizes as a protest. MISO states that the Commission did not receive any timely comments or protests in the proceeding and that the timely comments submitted to MISO during its stakeholder process were supportive of the proposed Tariff revisions. MISO claims that Exelon contacted MISO with shifting, after-the-stakeholder-meeting inquiries in late 2018 and that MISO sought, received, and responded to written comments from Exelon in January 2019. MISO argues that Exelon seeks to disrupt the process to revise the Tariff.[35]

26. MISO argues that while Exelon implies that the Commission should allow Exelon's late comments given the importance of the subject matter and the need to delve into various laws, Exelon's comments: lack any real legal citation related to

[32] Exelon Comments at 3-4.

[33] *Id.* at 4.

[34] *Id.* at 4-5.

[35] MISO Answer at 1-3.

cybersecurity besides general references to the FPA and the Critical Infrastructure Information Act of 2002, are vague and without proposed alternative Tariff language, and carelessly mischaracterize and/or misunderstand MISO's proposal and the existing provisions in the Tariff. MISO also claims that although Exelon was aware of the proposed changes, it did not actively participate in MISO's Reliability Subcommittee stakeholder meetings on the proposed Tariff changes. MISO asserts that Exelon's pre-filing communications regarding the use of legal authority were late, vague, and lacked alternative language options. MISO disagrees with Exelon's argument that information sharing should be limited to federal agencies in the energy sector, arguing that Exelon appears to suggest that MISO should not share information with the CFTC or Homeland Security.[36]

3. Deficiency Letter

27. In the Deficiency Letter, Commission staff inquired as to why MISO's proposed definition of Cyber Exigency was not limited to emergency-type situations. Commission staff also requested that MISO: (1) explain how it would determine which agencies have cybersecurity responsibilities to permit information sharing related to a Cyber Exigency, (2) detail the steps it intends to take to establish internal procedures to share information in response to a Cyber Exigency, (3) clarify what it intends to include in the mutual agreement to share information in response to a Cyber Exigency, and (4) explain what requirements would govern a federal agency or organization sharing information obtained from MISO related to a Cyber Exigency with a third party. Commission staff also asked MISO why it is necessary to harmonize the treatment of sharing confidential information with NERC and its Regional Entities with the treatment afforded to the Commission and other federal agencies. Commission staff also inquired why MISO finds that market participant notification is not necessary when disclosures are made to federal agencies other than the Commission or the CFTC.[37]

4. Deficiency Response

28. In its Deficiency Response, MISO clarifies its use of the term "exigency" compared to "emergency." MISO explains that the emphasis of the term "Emergency," as defined in the Tariff, is on an actual or imminent occurrence of traditional, adverse operating conditions (i.e., existing or impending loss of service due to severe weather conditions, fuel shortages, strikes, and other immediate threats to service).[38] In contrast,

---

[36] *Id.* at 3-6.

[37] Deficiency Letter at 2-3.

[38] Emergency is defined as: "(i) An abnormal system condition requiring manual or automatic action to maintain system frequency, or to prevent loss of firm Load, *(continued ...)*

MISO states that an exigency is an unforeseen occurrence or condition, which in this case would be the detected presence of a probed cyber intrusion or weakness in the electric utility infrastructure that calls for immediate action or remedy, possibly in the absence of any knowledge that immediate disruption in electrical service is threatened. Therefore, MISO argues that a Cyber Exigency is a more appropriate term because it would call for immediate action even if there is no immediate loss of service to customers.[39]

29. MISO states that it intends to work with Homeland Security on a pre-arranged basis.[40] MISO explains that Homeland Security and critical infrastructure entities developed a mutual agreement template entitled "Request for Technical Assistance," which identifies Homeland Security's legal authority mandating its cybersecurity responsibilities.[41] MISO states that its relevant staff has identified Homeland Security and the FBI as federal authorities with cybersecurity responsibilities and, although MISO only currently plans to have a mutual agreement with Homeland Security, a similar

---

equipment damage, or tripping of system elements that could adversely affect the reliability of any electric system or the safety of persons or property; (ii) fuel shortage requiring departure from normal operating procedures in order to minimize the use of such scarce fuel; or (iii) a condition that requires implementation of Emergency procedures as defined in this Tariff." Deficiency Response at 2 (citing MISO Tariff, Module A, Section 1 (Definitions)).

[39] *Id.* at 2-3.

[40] MISO reiterates that Presidential Executive Order No. 13800 (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure) tasked Homeland Security to coordinate with the Secretary of Defense, the Attorney General, the Director of National Intelligence, and the FBI Director with improving private-public coordination of efforts to improve cybersecurity. *Id.* at 4 (citing January 28 Filing, Transmittal at 2).

[41] MISO included a template "Request for Technical Assistance" as Tab A in its Deficiency Response. MISO states that Presidential Executive Order No. 13636 provides for Homeland Security, in coordination with relevant sector-specific federal agencies, to annually identify and maintain a list of critical infrastructure entities that meet specified criteria under section 9(a) of the executive order. These entities, which include MISO, are defined as those controlling "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." January 28 Filing, Transmittal at 2.

(continued ...)

process would be applied to identify any additional entities with whom MISO would enter into such a mutual agreement.[42]

30. MISO proposes additional revisions to Section 38.9.3.a.ii in the Tariff to clarify that MISO can share information in response to a Cyber Exigency with a federal agency that has cybersecurity responsibilities under federal laws and/or regulations for the protection of entities outside the federal agency itself. MISO argues that because legal authority may change with time under evolving federal attention to cybersecurity concerns, the proposed Tariff language avoids hardwiring agency names into the Tariff.[43]

31. MISO states that it intends to amend its Cyber-Security Incident Response Policy to recognize the Tariff revisions proposed in its Deficiency Response. MISO clarifies that its ability to activate the data sharing with Homeland Security would be limited, and the procedures that it would utilize regarding a request for assistance from Homeland Security are stated in the Request for Technical Assistance template with Homeland Security. MISO states that this mutually-agreed upon template contains MISO's understanding with Homeland Security related to the handling of shared information, including citations to relevant legal authority governing information sharing with Homeland Security. MISO states that it will use similar provisions in the event that it engages another federal agency in response to a Cyber Exigency. According to MISO, it can rapidly incorporate these changes into the Cyber-Security Incident Response Policy, and it will discuss such an incorporation with stakeholders at the next Reliability Subcommittee meeting following acceptance of the instant filing.[44]

32. Additionally, MISO states that the Request for Technical Assistance template contains the provisions regarding Homeland Security's treatment of confidential and non-public information shared under Section 38.9.3.a.ii of the Tariff. MISO explains that Homeland Security may share data submitted to it with U.S. Government entities with cybersecurity responsibilities; however, Homeland Security will follow requirements for sharing information so that it remains confidential and non-public.[45]

---

[42] Deficiency Response at 4.

[43] *Id.* at 5.

[44] *Id.* at 6.

[45] This includes any information that is exempt from disclosure under FOIA, consistent with 5 U.S.C. § 552 (b), including Exemption (b)(3) as specifically exempt from disclosure by statute, Exemption (b)(4) as trade secrets and commercial or financial

(continued ...)

33. With regard to harmonizing the treatment of the sharing of confidential information with NERC and its Regional Entities with the treatment afforded to the Commission and other federal agencies, MISO explains that the need for this harmonization relates to MISO's responsiveness to regulatory requirements and investigations that can be similar between the Commission and NERC and that this harmonized approach exists in other RTOs/ISOs.[46] MISO explains that both the Commission and NERC may audit MISO, may investigate matters raised by complaint or on their own initiative, and may assign penalties. According to MISO, during an investigation, the Commission and NERC may seek information; however, NERC's efforts to conduct confidential investigations may be undercut by a Tariff provision requiring market participant notification. Further, MISO argues that proposed Reliability Standard CIP-008-6 requires additional reporting of cyber-attacks, which, under the current Tariff language, could result in a wider dissemination of information than the proposed Tariff changes. MISO notes that such wider dissemination of information could result in alerting cyber-attacking perpetrators. Additionally, MISO notes that the treatment of information by NERC would be subject to the NERC Rules of Procedure for the protection of Confidential Information.[47]

34. With regard to market participant notification when MISO shares information with federal agencies other than the Commission and the CFTC, MISO proposes additional language in Section 38.9.3.a.ii to permit notification to the market participant, after consulting with the federal agency. MISO stresses that the information sharing in response to a Cyber Exigency requires different treatment than an operational emergency and may involve on-going, cooperative efforts to thwart cybersecurity threats confidentially. Therefore, MISO argues that it should consult with the federal agency involved to determine the specific timing for providing such notification and the extent to which such notification can be provided in order to preserve the reliability of the transmission system.[48]

---

information that is privileged or confidential, and Exemption (b)(7)(A)-(F) as records or information compiled for law enforcement purposes. *Id.* at 6-7.

[46] *Id.* at 7 & n.11.

[47] *Id.* at 7-8.

[48] *Id.* at 8-9.

III. Discussion

A. Procedural Matters

35. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2018), the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.

B. Substantive Matters

36. We accept MISO's proposed Tariff revisions, including those proposed in the Deficiency Response, effective March 30, 2019, as requested. We find that MISO's proposed Tariff revisions allow for greater information sharing with federal agencies with cybersecurity responsibilities in response to a Cyber Exigency while appropriately maintaining the confidentiality of non-public information of entities operating in MISO.

37. We disagree with Exelon's argument that MISO should limit the definition of Cyber Exigency to "emergency-type situations." In Order No. 848, the Commission highlighted the importance of reporting cybersecurity incidents, including "incidents that might facilitate subsequent efforts to harm the reliable operation of the [bulk electric system]."[49] We believe that, as proposed, the term Cyber Exigency will allow MISO to begin sharing information with the appropriate federal agencies before a potential cybersecurity threat becomes a cybersecurity incident or emergency.

38. We find that MISO has adequately responded to Exelon's request that MISO modify its proposal to narrow the agencies with which MISO may disclose information. In the changes to Section 38.9.3.a.ii proposed in the Deficiency Response, MISO proposes to only provide confidential information in response to a Cyber Exigency to a federal agency "that has cyber-security responsibilities under federal law and/or regulation for the protection of entities outside the federal agency itself."[50] This approach limits which federal agencies may receive confidential information to those with outward facing cybersecurity responsibilities, yet provides flexibility by avoiding the insertion of a static list of agencies into the Tariff that may become outdated.

39. We find that MISO's proposed information protection requirements in Section 38.9.3.b, in which MISO will require that any information provided to entities be treated as confidential and non-public, are just and reasonable. We therefore disagree with Exelon's request to enhance information protection requirements for any

[49] Order No. 848, 164 FERC ¶ 61,033 at P 1.

[50] Deficiency Response, Proposed Tariff, Module C, Section 38.9.3 (Disclosure to Specified Agencies/Organizations).

information shared with federal agencies. In particular, we disagree with Exelon's assertion that the provisions for disclosing information to the Commission and the CFTC are weakened by the proposal to require that the disclosure be "consistent with Applicable Laws and Regulations . . . ," rather than the existing Tariff language citing the precise regulations. Applicable Laws and Regulations is a defined term in MISO's Tariff, making it unnecessary to explicitly reference the statutory regimes under which information would be disclosed. Additionally, we find that MISO's mutual agreement with Homeland Security to share information in response to a Cyber Exigency, as proposed in Section 38.9.3.a.ii, does set protocols for the handling of any sharing of information with Homeland Security, which specifically references the FOIA exemption rules and the Cybersecurity Information Sharing Act of 2015. We note that MISO has committed to using this mutual agreement as a template for any federal agencies with whom it develops future information sharing capabilities in response to a Cyber Exigency.

40. In response to Exelon's request to enhance notification requirements, we find that MISO's proposed language in Section 38.9.3.a.ii strikes an appropriate balance between providing notification to an entity when its information is released to a federal agency while not encumbering MISO's ability to work with federal agencies to effectively respond to a Cyber Exigency. The proposed Tariff language provides for MISO, in consultation with the federal agency, to determine the appropriate notification, if any, on a case-by-case basis in order to maintain confidentiality of the agency's ongoing efforts to thwart any cybersecurity threats. We also note that aside from the case of a Cyber Exigency, as provided for in Section 38.9.3.a.ii, the existing notification requirements in Section 38.9.2 of the Tariff still apply and govern MISO's notification to an entity when any federal agency requests information.

41. With regard to Exelon's request that MISO establish internal procedures in advance of any incident, we note that MISO already plans to implement such procedures as explained in its deficiency response. Specifically, MISO states that it will amend its Cyber-Security Incident Response Policy to incorporate the proposed Tariff adjustments upon the Commission's acceptance of the instant filing and that MISO's mutual agreement with Homeland Security outlines the procedures that MISO will utilize to request assistance. MISO commits to using similar provisions in the event that it engages another federal agency in response to Cyber Exigency.

The Commission orders:

MISO's proposed Tariff revisions are hereby accepted, effective March 30, 2019, as discussed in the body of this order.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.