Memorandum

To: ISO Board of Governors

From: Roger Collanton VP, General Counsel and Chief Compliance Officer

Date: November 6, 2019

Re: **Decision on proposed cybersecurity tariff amendment**

This memorandum requires Board action.

EXECUTIVE SUMMARY

As the threat of cyberattacks on critical infrastructure continues to grow, the ISO should have the capability to seek assistance from federal agencies to investigate and thwart a serious attack on its systems that may affect grid reliability. The ISO proposes to amend the confidentiality provisions set forth in Section 20 of the tariff to allow the ISO, in the event of a cyberattack on its systems, to seek immediate assistance from federal agencies who have cybersecurity expertise (Homeland Security and FBI).

Management believes that these proposed amendments will allow federal agencies to provide necessary assistance to the ISO that will help counter a cyberattack to the ISO's systems while still preserving the confidentiality of any sensitive market participant information that these agencies access as part of their investigation. The ISO initiated a stakeholder process in August, and stakeholders support this proposal. Accordingly, Management recommends that the Board approve the proposal and recommends the following motion:

> ***Moved, that the ISO Board of Governors approves the cybersecurity tariff amendment proposal described in the memorandum dated November 6, 2019; and***
>
> ***Moved, that the ISO Board of Governors authorizes Management to make all necessary and appropriate filings with the Federal Energy Regulatory Commission to implement the proposal described in the memorandum, including any filings that implement the overarching initiative policy but contain discrete revisions to incorporate Commission guidance in any initial ruling on the proposed tariff amendment.***

DISCUSSION AND ANALYSIS

In recent years, cybersecurity concerns have led to the issuance of several Presidential Executive Orders designed, in part, to preserve the security of the electricity grid.[1] In response to these Executive Orders, the ISO proposes to amend its tariff to permit the ISO to share confidential information in response to a "cyber exigency" with any federal agency with cybersecurity responsibilities, such as Homeland Security or the FBI.[2] Cyber exigency is defined as a suspicious electronic act or event that has the potential to compromise the ongoing operation of the CAISO, the CAISO Markets, or reliability within the ISO balancing authority area or other electrical facilities directly or indirectly connected to the ISO controlled grid and whose severity reasonably requires that the ISO obtain expert assistance from federal agencies not normally called upon to counter such an electronic act or to resolve such an event.

Should a cyber exigency occur, the ISO will have sole discretion to ask federal agencies to help investigate and thwart the attack. The ISO also will have full control over the time and scope of the agencies' access to the ISO's systems. In addition, the ISO will not share confidential market participant information with any federal agency without prior agreement with that agency regarding the terms under which information sharing would occur. Any resulting data sharing will be limited, and only as necessary to assist with the cyber exigency.

To this end, the ISO intends to work with Homeland Security on a pre-arranged basis. In 2018, Homeland Security and critical infrastructure entities, including the ISO, developed an agreement template entitled "Request for Technical Assistance," which identifies Homeland Security's legal authority mandating its cybersecurity responsibilities. The ISO has identified Homeland Security and the FBI as federal authorities with cybersecurity responsibilities and, although the ISO only currently plans to have an agreement with Homeland Security, a similar process would be applied to identify any additional entities with whom the ISO would enter into such a mutual agreement. The "Request for Technical Assistance" agreement includes protocols for the handling of any sharing of information with Homeland Security, and specifically

[1] 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 the ISO. 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 the ISO.

[2] Midcontinent Independent System Operator (MISO) completed a similar stakeholder proposal this year, and FERC approved analogous changes to the MISO tariff on June 20, 2019 (Order on Proposed Tariff Revisions, 167 FERC ¶ 61,229 (2019)).

references the Freedom of Information Act exemption rules and the Cybersecurity Information Sharing Act of 2015.

The proposed amendments also require the ISO to notify market participants in the event these federal agencies receive a third party request to disclose any non-public information they obtained during their investigation. This is similar to existing language in the tariff that applies when the ISO receives a request by FERC or the CFTC to share non-public information that has been shared with those agencies with third parties.[3] Here, should the ISO receive a request from Homeland Security to disclose non-public market participant information to third parties, the ISO will notify the affected market participants by appropriate means based on the individual circumstances (e.g., time requirements, breadth of persons affected, and information requested) to give both the ISO and the market participants the opportunity to respond before the information is shared with the third party.

In sum, this proposal will allow the ISO to seek immediate assistance from appropriate federal agencies in the event of a cyber exigency. The ISO will retain sole discretion over whether to enlist the agencies' help and the scope of the agencies' access to its systems during a resulting investigation. Should these agencies access confidential market participant information in the course of their investigation, they will be obligated to protect the confidentiality of that information, and the proposed amendments set forth a clear process that allows the ISO, and any affected market participant, to object to the sharing of the information in response to a future third party data request.

CONCLUSION

Management recommends that the Board approve the proposal as outlined in this memorandum that will allow the ISO to receive immediate assistance from federal agencies in the event of a cyber exigency involving its systems.

[3] Section 20.4(c)(i) of the ISO tariff currently allows the ISO to disclose confidential information with certain federal agencies (FERC and CFTC) during an investigation, without prior notice to an affected market participant.