California ISO

Critical Infrastructure and Cyber Security

White Paper

August 21, 2019

Table of Contents

1. Summary

The CAISO proposes to amend its tariff to enhance its ability to coordinate with federal agencies in cybersecurity emergencies. CAISO tariff section 20.4(c) currently allows the CAISO to disclose confidential or commercially sensitive information, without notice to an affected Market Participant, with the Federal Energy Regulatory Commission (FERC) and the Commodity Futures Trading Commission (CFTC) and their staff during an investigation. While retaining FERC's and CFTC's ability to request and receive non-public information, the CAISO proposes to add a new provision within Section 20.4(c) to authorize the CAISO to provide information to other federal agencies and organizations that have cybersecurity responsibilities in response to a "Cyber Exigency."

The CAISO also proposes to amend Appendix A of its tariff to define the new term, "Cyber Exigency."

2. Stakeholder Engagement Plan

Date	Milestone
August 21, 2019	**White paper and tariff amendment posted**
September 4	**Comments due on white paper and tariff amendment**
September 11	**Conference call**
No later than October 15	**File tariff amendment with FERC**

3. Background

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 CAISO.[1] 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

[1] Executive Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11,739 (February 19, 2013).

that agencies could employ to support cybersecurity efforts of certain entities, such as the CAISO.[2]

In response to these Executive Orders, the CAISO proposes to amend its tariff to permit the CAISO to share information in response to a Cyber Exigency with any federal agency with cybersecurity responsibilities, such as Homeland Security or the FBI.[3] Information sharing will occur *only* in situations that involve a Cyber Exigency. The CAISO will be under *no* obligation to provide information to these federal agencies, although it may seek help under severe circumstances. The CAISO does not intend to share information with any federal agency without prior mutual agreement regarding the terms under which data sharing would occur, and any data sharing will be limited.

To this end, the CAISO intends to work with Homeland Security on a pre-arranged basis. Homeland Security and critical infrastructure entities, including the CAISO, developed a mutual agreement template entitled "Request for Technical Assistance," which identifies Homeland Security's legal authority mandating its cybersecurity responsibilities. The CAISO has identified Homeland Security and the FBI as federal authorities with cybersecurity responsibilities and, although the CAISO only currently plans to have a mutual agreement with Homeland Security, a similar process would be applied to identify any additional entities with whom the CAISO 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 references the Freedom of Information Act exemption rules and the Cybersecurity Information Sharing Act of 2015.

The CAISO's tariff proposal also includes language regarding the notification of market participants that currently applies when the CAISO receives a request by FERC or the CFTC to share non-public information with third parties. Accordingly, should the CAISO receive a request from Homeland Security to share non-public information with third parties, the CAISO will notify the affected market participants by appropriate means based on the individual circumstances of each situation (e.g., time requirements, breadth of persons affected, and information requested) to give both the CAISO and market participants the opportunity to respond before the information is made public.

Finally, the CAISO proposes to include "Cyber Exigency" as a new term within Appendix A of its tariff. The CAISO believes the term "Cyber Exigency" is appropriate because 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

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

[3] 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)).

infrastructure that calls for immediate action or remedy, possibly in the absence of any knowledge that immediate disruption in electrical service is threatened.

4. Proposed Resolution

The CAISO proposes to modify CAISO tariff section 20.4(c) to permit the CAISO to share non-public information with federal agencies that have cybersecurity responsibilities.

20.4 Disclosure

Notwithstanding anything in this Section to the contrary,

* * * * *

(c) The CAISO may disclose confidential or commercially sensitive information without notice to an affected Market Participant, in the following circumstances:

(i) If the FERC, the Commodity Futures Trading Commission ("CFTC"), or the staff of one of those agencies, during the course of an investigation or otherwise, requests information that is confidential or commercially sensitive. In providing the information to FERC or its staff, the CAISO shall take action consistent with 18 C.F.R. §§ 1b.20 and 388.112, or to the CFTC or its staff, the CAISO shall take action consistent with 17 C.F.R. §§ 11.3 and 145.9, and request that the information be treated as confidential and non-public by the agency and its staff and that the information be withheld from public disclosure. The CAISO shall provide the requested information to the agency or its staff within the time provided for in the request for information. The CAISO shall notify an affected Market Participant within a reasonable time after the CAISO is notified by the agency or its staff that a request for disclosure of, or decision to disclose, the confidential or commercially sensitive information has been received, at which time the CAISO and the affected Market Participant may respond before such information would be made public; or

(ii) If the National Cyber Communication Information Center ("NCCIC," part of the Department of Homeland Security), or a federal agency with similar cybersecurity responsibilities, or the staff of one of those agencies, requests information that is confidential or commercially sensitive in response to a Cyber Exigency that threatens or has the potential to threaten reliable operation of the CAISO Balancing Authority Area. In providing the information to

the agency or its staff, the CAISO shall take action consistent with applicable laws and regulations, as well as other applicable policies or procedures of the agency, and request that the information be treated as confidential and non-public by the agency and its staff and that the information be withheld from public disclosure. The CAISO shall notify an affected Market Participant within a reasonable time after the CAISO is notified by the agency or its staff that a request for disclosure of, or decision to disclose, the confidential or commercially sensitive information has been received, at which time the CAISO and the affected Market Participant may respond before such information would be made public; or

(iii) In order to maintain reliable operation of the CAISO Balancing Authority Area, the CAISO may share critical operating information, system models, and planning data with the WECC Reliability Coordinator that has executed the Western Electricity Coordinating Council Confidentiality Agreement for Electric System Data, or is subject to similar confidentiality requirements; or

(iv~~ii~~) In order to maintain reliable operation of the CAISO Balancing Authority Area, the CAISO may share individual Generating Unit Outage information with the operations engineering and the outage coordination division(s) of other Balancing Authorities, Participating TOs, MSS Operators and other transmission system operators engaged in the operation and maintenance of the electric supply system whose system is significantly affected by the Generating Unit and who have executed the Western Electricity Coordinating Council Confidentiality Agreement for Electric System Data; or ~~.~~

(~~i~~v) In order to maintain reliable operation of the CAISO Balancing Authority Area, the CAISO may share information regarding Maintenance Outages and Forced Outages of natural gas-fired generation resources and Maintenance Outages and Forced Outages of elements of the ISO Controlled Grid with natural gas transmission and distribution utilities operating inter-state and/or intra-state natural gas pipelines that serve natural gas-fired generation resources within the CAISO Balancing Authority Area. The CAISO may share information necessary for day-to-day coordination and longer term planning of gas transmission and pipeline outages which information includes, but is not limited to, the identity of individual natural gas-fired generation resources that

are needed to support reliability of the ISO Balancing Authority Area in the event of natural gas shortage, natural gas pipeline testing and maintenance, or other curtailment of natural gas supplies. The information will be shared only pursuant to a non-disclosure agreement and non-disclosure statement included as part of the Business Practice Manual.

* * * * *

Appendix A

Master Definitions Supplement

* * * * *

- Cyber Exigency

A suspicious electronic act or event that has the potential to compromise reliability within the CAISO Balancing Authority Area or other electrical facilities directly or indirectly connected to the CAISO Controlled Grid and whose severity reasonably requires that the CAISO obtain expert assistance not normally called upon to counter such an electronic act or to resolve such an event.

* * * * *

5. Next Steps

The CAISO will request that these modifications become effective December 15, 2019.

The CAISO will discuss this white paper and the proposed tariff amendments with stakeholders during a conference call on September 11, 2019. Stakeholders are asked to submit written comments by September 4, 2019 to initiativecomments@caiso.com.