November 22, 2019

The Honorable Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Re: California Independent System Operator Corporation
CAISO Tariff Amendment to Facilitate Data Sharing in Response to a Cyber Exigency

Docket No. ER20-___-000

Dear Secretary Bose:

The California Independent System Operator Corporation ("CAISO") proposes this CAISO tariff amendment to allow for the sharing of confidential data with certain federal agencies in the event of a cyberattack on CAISO systems.[1] To allow for this data sharing, the CAISO proposes a new provision specific to the sharing of confidential information with federal agencies who have cybersecurity responsibilities, without notice to affected market participants, in the event of a "Cyber Exigency" and a new definition for the term "Cyber Exigency".[2]

The proposed tariff amendment promotes reliability by allowing federal agencies with cybersecurity expertise the ability, upon the CAISO's request, to immediately assist the CAISO in investigating and thwarting a cyberattack that may compromise the CAISO's operations, markets, or the integrity of the grid ("Cyber Exigency"), without having to first give notice to affected market participants whose information may be exposed during the investigation. In addition, the amendment contains a process for ensuring that market participants, whose confidential data would be exposed, have the opportunity to object to a third party request for the participants' information. The CAISO respectfully requests that the Commission accept this amendment to the CAISO tariff effective February 5, 2020.

[1] The CAISO submits the proposed tariff changes pursuant to Section 205 of the Federal Power Act, 16 U.S.C. § 824d.

[2] Capitalized terms not otherwise defined in this filing have the meanings set forth in Appendix A to the CAISO tariff as revised by this filing, and references to numbered sections are references to sections of the CAISO tariff as revised by this tariff filing, unless the context indicates otherwise.

I. Background

In recent years, cybersecurity concerns have led to the issuance of several Presidential Executive Orders ("Executive Orders") related to the protection of critical infrastructure. 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.[3] 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 CAISO.[4]

To this end, Homeland Security and critical infrastructure entities, including the CAISO, developed a mutual agreement template in 2018 entitled "Request for Technical Assistance," which identifies Homeland Security's legal authority mandating its cybersecurity responsibilities. This 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 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.

II. Proposed Amendment to CAISO Tariff

The CAISO proposes to amend its tariff so it may share confidential information with certain federal agencies, without prior notice to affected market participants, in the event of a Cyber Exigency on CAISO's systems.[5] CAISO

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

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

[5] Marked proposed revisions to CAISO tariff section 20.4(c) and Appendix A are included as Attachment B.

tariff section 20.4(c) currently allows the CAISO to disclose confidential information, without notice to an affected market participant, with the Commission 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.

CAISO proposes to define a "Cyber Exigency" in Appendix A of its tariff 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 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 from federal agencies not normally called upon to counter such an electronic act or to resolve such an event."[6]

The proposed amendment to Section 20.4(c) of the CAISO tariff will allow the CAISO to share confidential information, without having to first give notice to affected market participants, if Homeland Security (or a federal agency with similar cybersecurity responsibilities) requests access to such information during a Cyber Exigency.[7] As a result, this proposed revision would allow the CAISO to seek immediate assistance from a federal agency with cybersecurity expertise and allow such agency to access the CAISO's systems to investigate and thwart the attack in an effort to maintain reliable operation of CAISO, its markets, and its balancing authority area.

Notwithstanding the proposed allowance, the CAISO is not under an obligation to seek federal agency assistance in the event of a Cyber Exigency. Should it choose to do so, however, the CAISO will have control over the time and scope of Homeland Security's access to the CAISO's systems, consistent with the terms set forth in the "Request For Technical Assistance" document. The CAISO will not share confidential market participant information with a federal agency without prior agreement with that agency regarding the terms under which information sharing would occur (e.g., the "Request For Technical Assistance" document already in place with Homeland Security). Any resulting data sharing will be limited, and only as necessary to assist in responding to the Cyber Exigency.

Should Homeland Security or other agency access confidential or commercially sensitive information of a market participant during its investigation,

---

6 Id.

7 Id.

the proposed tariff revision requires the CAISO to request that Homeland Security treat such information as confidential and that the information be withheld from public disclosure.[8]

Finally, the proposed tariff revision requires the CAISO to notify an affected market participant in the event Homeland Security receives a third party request to disclose any non-public information the agency obtained during its investigation (e.g., a third party request under the Freedom of Information Act).[9] The proposed tariff language is similar to existing language in tariff Section 20.4(c)(i) that applies when the CAISO receives a request by FERC or the CFTC to share non-public information that has been shared with those agencies with third parties. Here, should the CAISO receive a request from Homeland Security to disclose non-public market participant information to third parties, the CAISO 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 CAISO and the market participants the opportunity to respond before the information is shared with the third party.

III. Stakeholder Process

On August 21, 2019, the CAISO published a draft proposal to its stakeholders, detailing the proposed amendment to Section 20 and Appendix A of its tariff. The CAISO hosted a public call on September 11, 2019 to discuss the proposal. Based on stakeholder input, the CAISO published draft final tariff revisions on November 5, 2019. All stakeholders involved support this proposal. The proposal was approved by the CAISO Board of Governors on November 13, 2019.

IV. Effective Date

The CAISO respectfully requests that the Commission accept the proposed tariff amendment, effective February 5, 2020.

V. Service

The CAISO has served copies of this filing upon the California Public Utilities Commission, the California Energy Commission, and all parties with scheduling coordinator agreements under the CAISO tariff. In addition, the CAISO has posted the filing on the CAISO website.

[8] Id.

[9] Id.

VI. Contents of Filing

In addition to this transmittal letter, this filing includes the following attachments:

Attachment A	Clean tariff sheets with a requested effective date of February 5, 2020;
Attachment B	Marked tariff sheets with a requested effective date of February 5, 2020;
Attachment C	Stakeholder Proposal; and
Attachment D	CAISO Board of Governors Memorandum and Board Resolution.

VII. Correspondence

Pursuant to Rule 203(b) of the Commission's Rules of Practice and Procedure,[10] the CAISO requests that all correspondence, pleadings, and other communications concerning this filing be served upon the following:

John E. Spomer
Senior Counsel
California Independent System
Operator Corporation
250 Outcropping Way
Folsom, CA 95630
Tel: (916) 608-7287
E-mail: jspomer@caiso.com

[10] 18 C.F.R. § 385.203(b).

VIII. Conclusion

The CAISO requests that the Commission accept the amendment proposed in this filing effective February 5, 2020 as requested. If there are any questions concerning this filing, please contact the undersigned.

Respectfully submitted,

By: */s/ John E. Spomer*

Roger E. Collanton
General Counsel
John C. Anders
Assistant General Counsel
John E. Spomer
Senior Counsel
California Independent System
Operator Corporation
250 Outcropping Way
Folsom, CA 95630

Attorneys for the California Independent System Operator Corporation

Attachment A

Clean Tariff

Tariff Amendment to Facilitate Data Sharing in Response to a Cyber Exigency

California Independent System Operator Corporation

November 22, 2019

20.4 Disclosure

Notwithstanding anything in this Section 20 to the contrary,

(a) The CAISO: (i) shall publish individual bids ninety (90) days after the Trading Day with respect to which the bid was submitted and in a manner that does not reveal the specific resource or the name of the Scheduling Coordinator submitting the bid, but that allows the bidding behavior of individual, unidentified resources and Scheduling Coordinators to be tracked over time; (ii) may publish data sets analyzed in any public report issued by the CAISO or by the MSC, provided that such data sets shall be published no sooner than six (6) months after the latest Trading Day to which data in the data set apply, and in a manner that does not reveal any specific resource or the name of any Scheduling Coordinator submitting bids included in such data sets; and (iii) shall, consistent with 18 CFR § 35.28 (g)(4), electronically deliver to FERC, on an ongoing basis and in a form and manner consistent with the CAISO's own collection of data and in a form and manner acceptable to FERC, data related to the CAISO Markets.

(b) If the CAISO is required by applicable laws or regulations, or in the course of administrative or judicial proceedings, to disclose information that is otherwise required to be maintained in confidence pursuant to this Section 20, the CAISO may disclose such information; provided, however, that as soon as the CAISO learns of the disclosure requirement and prior to making such disclosure, the CAISO shall notify any affected Market Participant of the requirement and the terms thereof. The Market Participant may, at its sole discretion and own cost, direct any challenge to or defense against the disclosure requirement and the CAISO shall cooperate with such affected Market Participant to the maximum extent practicable to minimize the disclosure of the information consistent with applicable law. The CAISO shall cooperate with the affected Market Participant to obtain proprietary or confidential treatment of confidential information by the person to whom such information is disclosed prior to any such disclosure.

(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) 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

(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.

(d) Notwithstanding the provisions of Section 20.2(e), information submitted through Resource Adequacy Plans and Supply Plans in accordance with Section 40 may be provided to:

(i) the Scheduling Coordinator(s) and/or Market Participant(s) involved in a dispute or discrepancy as to whether a resource is properly identified in a Resource Adequacy Plan or a Supply Plan only to the limited extent necessary to identify the disputed transaction and the relevant counterparty or counterparties.

(ii) the regulatory entity, whether the CPUC, other Local Regulatory Authority, or federal agency, with jurisdiction over a Load Serving Entity involved in a dispute or discrepancy as to whether a resource is properly identified in a Resource Adequacy Plan or the Supply Plan, or otherwise identified by the CAISO as exhibiting a potential deficiency in demonstrating compliance with resource adequacy requirements adopted by the CPUC, other Local Regulatory Authority, or federal agency, as applicable. The information provided shall be limited to the particular dispute, discrepancy, or deficiency.

(iii) the California Energy Commission with respect to Demand Forecast information provided to the CAISO under Sections 40.2.2.3 and 40.2.3.3(b) to the extent the CAISO seeks, and the California Energy Commission grants, confidential treatment of such information pursuant to California Public Resources Code Section 25322 and related regulations.

(e) Notwithstanding the provisions of Section 20.2(f), information submitted through the Transmission Planning Process shall be disclosed as follows:

(i) Critical Energy Infrastructure Information may be provided to a requestor where such person is employed or designated to receive CEII by: (a) a Market

Participant; (b) an electric utility regulatory agency within California; (c) an Interconnection Customer that has submitted an Interconnection Request to the CAISO under the CAISO's Large Generator Interconnection Procedure or Small Generator Interconnection Procedure (LGIP or SGIP); (d) a developer having a pending or potential proposal for development of a Generating Facility or transmission addition, upgrade or facility and that is performing studies in contemplation of filing an Interconnection Request or submitting a transmission infrastructure project through the CAISO Transmission Planning Process; or (e) a not-for-profit organization representing consumer regulatory or environmental interests before a Local Regulatory Authority or federal regulatory agency. To obtain Critical Energy Infrastructure Information, the requestor must submit a statement as to the need for the CEII, and must execute and return to the CAISO the form of the non-disclosure agreement and non-disclosure statement included as part of the Business Practice Manual. The CAISO may, at its sole discretion, reject a request for CEII and, upon such rejection, the requestor will be directed to utilize the FERC procedures for access to the requested CEII.

(ii) Information that is confidential under Section 20.2(f)(i) or 20.2.(f)(ii) may be disclosed to any individual designated by a Market Participant, electric utility regulatory agency within California, or other stakeholder that signs and returns to the CAISO the form of the non-disclosure agreement, nondisclosure statement and certification that the individual is a non-Market Participant, which is any person or entity not involved in a marketing, sales, or brokering function as market, sales, or brokering are defined in FERC's Standards of Conduct for Transmission Providers (18 C.F.R. § 358 et seq.), included as part of the Business Practice Manual; provided, however, that information obtained pursuant to this Section 20.4(e)(ii) will be provided only in composite form so that information related to individual Load Serving Entities or Scheduling Coordinators will not be disclosed.

(iii) Data base and other transmission planning information obtained from the WECC, or its successor, may be disclosed to individuals designated by a Market Participant, electric utility regulatory agency within California, or other stakeholder in accordance with the procedures set forth in the Business Practice Manual.

Nothing in this Section 20 shall limit the ability of the CAISO to aggregate data for public release about the adequacy of supply.

*** * * * ***

Appendix A

Master Definitions Supplement

*** * * * ***

- Cyber Exigency

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 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 from federal agencies not normally called upon to counter such an electronic act or to resolve such an event.

*** * * * ***

Attachment B

Marked Tariff

Tariff Amendment to Facilitate Data Sharing in Response to a Cyber Exigency

California Independent System Operator Corporation

November 22, 2019

20.4 Disclosure

Notwithstanding anything in this Section 20 to the contrary,

(a) The CAISO: (i) shall publish individual bids ninety (90) days after the Trading Day with respect to which the bid was submitted and in a manner that does not reveal the specific resource or the name of the Scheduling Coordinator submitting the bid, but that allows the bidding behavior of individual, unidentified resources and Scheduling Coordinators to be tracked over time; (ii) may publish data sets analyzed in any public report issued by the CAISO or by the MSC, provided that such data sets shall be published no sooner than six (6) months after the latest Trading Day to which data in the data set apply, and in a manner that does not reveal any specific resource or the name of any Scheduling Coordinator submitting bids included in such data sets; and (iii) shall, consistent with 18 CFR § 35.28 (g)(4), electronically deliver to FERC, on an ongoing basis and in a form and manner consistent with the CAISO's own collection of data and in a form and manner acceptable to FERC, data related to the CAISO Markets.

(b) If the CAISO is required by applicable laws or regulations, or in the course of administrative or judicial proceedings, to disclose information that is otherwise required to be maintained in confidence pursuant to this Section 20, the CAISO may disclose such information; provided, however, that as soon as the CAISO learns of the disclosure requirement and prior to making such disclosure, the CAISO shall notify any affected Market Participant of the requirement and the terms thereof. The Market Participant may, at its sole discretion and own cost, direct any challenge to or defense against the disclosure requirement and the CAISO shall cooperate with such affected Market Participant to the maximum extent practicable to minimize the disclosure of the information consistent with applicable law. The CAISO shall cooperate with the affected Market Participant to obtain proprietary or confidential treatment of confidential information by the person to whom such information is disclosed prior to any such disclosure.

(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

(~~iii~~iv) 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.

(d) Notwithstanding the provisions of Section 20.2(e), information submitted through Resource Adequacy Plans and Supply Plans in accordance with Section 40 may be provided to:

(i) the Scheduling Coordinator(s) and/or Market Participant(s) involved in a dispute or discrepancy as to whether a resource is properly identified in a Resource Adequacy Plan or a Supply Plan only to the limited extent necessary to identify the disputed transaction and the relevant counterparty or counterparties.

(ii) the regulatory entity, whether the CPUC, other Local Regulatory Authority, or federal agency, with jurisdiction over a Load Serving Entity involved in a dispute or discrepancy as to whether a resource is properly identified in a Resource Adequacy Plan or the Supply Plan, or otherwise identified by the CAISO as exhibiting a potential deficiency in demonstrating compliance with resource adequacy requirements adopted by the CPUC, other Local Regulatory Authority, or federal agency, as applicable. The information provided shall be limited to the particular dispute, discrepancy, or deficiency.

(iii) the California Energy Commission with respect to Demand Forecast information provided to the CAISO under Sections 40.2.2.3 and 40.2.3.3(b) to the extent the CAISO seeks, and the California Energy Commission grants, confidential treatment of such information pursuant to California Public Resources Code Section 25322 and related regulations.

(e) Notwithstanding the provisions of Section 20.2(f), information submitted through the Transmission Planning Process shall be disclosed as follows:

(i) Critical Energy Infrastructure Information may be provided to a requestor where such person is employed or designated to receive CEII by: (a) a Market

Participant; (b) an electric utility regulatory agency within California; (c) an Interconnection Customer that has submitted an Interconnection Request to the CAISO under the CAISO's Large Generator Interconnection Procedure or Small Generator Interconnection Procedure (LGIP or SGIP); (d) a developer having a pending or potential proposal for development of a Generating Facility or transmission addition, upgrade or facility and that is performing studies in contemplation of filing an Interconnection Request or submitting a transmission infrastructure project through the CAISO Transmission Planning Process; or (e) a not-for-profit organization representing consumer regulatory or environmental interests before a Local Regulatory Authority or federal regulatory agency. To obtain Critical Energy Infrastructure Information, the requestor must submit a statement as to the need for the CEII, and must execute and return to the CAISO the form of the non-disclosure agreement and non-disclosure statement included as part of the Business Practice Manual. The CAISO may, at its sole discretion, reject a request for CEII and, upon such rejection, the requestor will be directed to utilize the FERC procedures for access to the requested CEII.

(ii) Information that is confidential under Section 20.2(f)(i) or 20.2.(f)(ii) may be disclosed to any individual designated by a Market Participant, electric utility regulatory agency within California, or other stakeholder that signs and returns to the CAISO the form of the non-disclosure agreement, nondisclosure statement and certification that the individual is a non-Market Participant, which is any person or entity not involved in a marketing, sales, or brokering function as market, sales, or brokering are defined in FERC's Standards of Conduct for Transmission Providers (18 C.F.R. § 358 et seq.), included as part of the Business Practice Manual; provided, however, that information obtained pursuant to this Section 20.4(e)(ii) will be provided only in composite form so that information related to individual Load Serving Entities or Scheduling Coordinators will not be disclosed.

(iii) Data base and other transmission planning information obtained from the WECC, or its successor, may be disclosed to individuals designated by a Market Participant, electric utility regulatory agency within California, or other stakeholder in accordance with the procedures set forth in the Business Practice Manual.

Nothing in this Section 20 shall limit the ability of the CAISO to aggregate data for public release about the adequacy of supply.

* * * * *

Appendix A

Master Definitions Supplement

* * * * *

- Cyber Exigency

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 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 from federal agencies not normally called upon to counter such an electronic act or to resolve such an event.

* * * * *

Attachment C

Stakeholder Proposal

Tariff Amendment to Facilitate Data Sharing in Response to a Cyber Exigency

California Independent System Operator Corporation

November 22, 2019

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.

Attachment D

CAISO Board of Governors Memorandum and Board Resolution

Tariff Amendment to Facilitate Data Sharing in Response to a Cyber Exigency

California Independent System Operator Corporation

November 22, 2019

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.

Board of Governors **November 13, 2019**

Decision on proposed cyber security tariff amendment

General Session

Motion

Moved, that the ISO Board of Governors approves the cyber security 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.

Moved: Olsen **Second: Bhagwat**

Board Action: **Passed** Vote Count: **5-0**	
Bhagwat	Y
Borenstein	Y
Galiteva	Y
Leslie	Y
Olsen	Y

Motion Number: 2019-11-G4