California ISO

September 12, 2019

Response to Stakeholder Comments on Draft Tariff Language
Critical Infrastructure and Cyber Security

Tariff Section	Stakeholder Comment	ISO Response
20.4(c)(ii)	The Six Cities[1] proposes the following edits: "…in response to a Cyber Exigency ~~that threatens or has the potential to threaten reliable operation of the CAISO Balancing Authority Area~~, provided that the information requested is reasonably related to investigation or resolution of the Cyber Exigency." The Six Cities comments that if the definition of "Cyber Exigency" is revised (see proposed revisions below), language is redundant.	See response below.
20.4(c)(ii)	The Six Cities requests that the ISO specify that the information to be provided should be related to the Cyber Exigency.	In the event of a Cyber Exigency, the ISO may need to allow the DHS access to all of its systems to locate and thwart the attack. Accordingly, we do not believe it is possible to limit the information provided only to that which is related to the exigency.
20.4(c)(iii)	The Six Cities questions if the reference to the "WECC Reliability Coordinator" is still relevant. The Six Cities asks if the language should be modified to reference information sharing with "other Reliability Coordinators?"	The ISO intends to modify this language in an upcoming tariff clean up filing with FERC.

[1] The Six Cities is comprised of the Cities of Anaheim, Azusa, Banning, Colton, Pasadena, and Riverside, California.

Tariff Section	Stakeholder Comment	ISO Response
Definition of Cyber Exigency	The Six Cities proposes the following edits to the definition of "Cyber Exigency": "A suspicious act or event that has the potential to materially compromise or does materially compromise the reliability or operability of ~~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 electric act or to resolve such an event~~.	See response below.
Definition of Cyber Exigency	The Six Cities proposes that the ISO delete reference to the CAISO's need for "expert assistance." The Six Cities states that it is not obvious why the level or type of resources needed by the CAISO to address a Cyber Exigency is linked to the CAISO's willingness to respond to agency requests for information about the Cyber Exigency. The Six Cities states that a preferable approach would be to focus on events that "materially" compromise reliability or operability within the CAISO Balancing Authority Area (or have the potential to do so).	The ISO prefers to keep the "expert assistance" condition within the definition of Cyber Exigency. In doing so, it ensures that federal government agencies will only get involved if the cyber attack is so extreme as to require the help of DHS, FBI, etc. Less significant attempts at attacking the ISO's systems can be handled by the ISO's information security team without government assistance. However, in order to clarify that this "expert assistance" will come from federal agencies (and not from, for example, private contractors), the ISO will modify the language in the definition to read: "…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." With respect to the proposed condition that the event must "materially" compromise reliability, the ISO

Tariff Section	Stakeholder Comment	ISO Response
		prefers to keep the definition of Cyber Exigency more generic, rather than inserting the proposed qualifying language. Bear in mind that this definition contains substantially the same language that MISO included in its definition of Cyber Exigency, which has already been accepted by FERC. For sake of consistency among all ISOs/RTOs going forward, the ISO prefers to keep the definition as uniform as possible.