

ATTACHMENT A2

December 4, 2020, First Revision Implemented

June 24, 2020, Initial Version Implemented

Interim Trial Procedures for Exchange of Sensitive Information

Preface

In administering the new Physical Security requirements, Safety Policy Division (SPD) and IOU staff jointly proposed to test procedures for IOU sharing of sensitive data according to a Five-step Process (detailed below). The initial proposed Interim Trial Procedures (or ITPs), effective June 24, 2020, were tested over the course of a review cycle of IOU Physical Security work products -- the Preliminary Assessments, due July 10, 2020. That exercise yielded findings with which to improve the ITPs, and we here address identified deficiencies via our revisions. The original purposes assigned to the ITPs remain unchanged. ITPs are expected to require reduced staff resources while satisfying concerns raised by IOU staff, namely custody and protection of information thought to rise to a level of national security interests. As with all information categorized as restricted to the public, utilities would be obligated to justify categorizing data as sensitive, and therefore shall submit at the time a work product is provided to the Commission, a signed declaration supporting confidential designation and justifying the data as secret and protected.¹

The ITPs are necessary because the Commission requires certain information from the utilities to enable the Commission to perform its regulatory oversight functions. The IOUs and the Commission recognize that the sharing of “security sensitive” information raises potential security risks, particularly when the practice is conducted remotely and facilitated by technology. It is for this reason that adherence to the ITPs and their provisions for remote data access is so vital.

Provisions Surrounding Interim Trial Procedures

IOU Core Work Products Subject to Interim Trial Procedures (ITPs)

(D.19-01-018 OP 1) | Preliminary Assessments include a list of covered priority facilities subject to security plans; and site, risk, and threat assessments. Preliminary Assessments consist of all analysis up to but short of identification of mitigation measures. Due July 10, 2020

(D.19-01-018 OP 2) | Final Security Plan Reports are blanket reports submitted for each IOU’s set of covered facilities that include a list of potential and recommended mitigation measures, an identified “preferred alternative” that consists of a set of mitigation measures that the IOU supports

¹ Physical facility, cyber-security sensitive, or critical energy infrastructure data, including without limitation critical energy infrastructure information (CEII) as defined by the regulations of the Federal Energy Regulatory Commission at 18 C.F.R. § 388.113 (Protected under Govt. Code § 6254(k), (ab); 6 U.S.C. § 131; 6 CFR § 29.2)

implementing, a statement of “response to recommendations” that has the IOU justify any consultant-recommended mitigation measures that the IOU declines. Due July 10, 2021

(D.19-01-018 OP 25) | Program Review and Five-year Plan Update. Due August 10, 2026 (approx.)

IOU Ongoing Work Products Not Routinely Subject to Interim Trial Procedures (ITPs)

(D.19-01-018 OP 29²) | U.S. DOE OE-417 Reports of disruption and security incidents are not considered highly sensitive data that rises to a level of national security interests. Thus, for their routine submittal to the Commission they are not bound by this set of ITPs. However, should there be an emergency event that requires briefing the Commission on an event that triggers OE-417 reporting, the ITPs could serve as a means of conferencing. OE-417 Reports in unredacted format shall be considered confidential information subject to exclusion from public disclosure provisions.

(D.19-01-018 OP 31) | Annual Reports are not considered highly sensitive data that rises to a level of national security interests. Thus, for their routine submittal to the Commission they are not bound by this set of ITPs. However, should there be an emergency event that requires briefing the Commission on an event captured in an Annual Report, the ITPs could serve as a means of conferencing. OE-417 Reports in unredacted format shall not be considered confidential information subject to exclusion from public disclosure provisions. Public versions of the Annual Reports, as stipulated by P.U. Code Sec. 590, are required to be made available to the public. Due March 31, 2020, and annually thereafter. Additionally, Annual Reports in unredacted format shall not be considered confidential information subject to exclusion from public disclosure provisions.

IOU Ongoing Work Products Generated at Request of Commission Staff (Data Requests)

Commission data requests to utilities rarely entail highly sensitive data that rises to a level of national security interests. Thus, for their routine submittal to the Commission they are not bound by this set of ITPs. However, it’s foreseeable that there may come a time when the Commission will need to request such data for the purposes of carrying out regulatory oversight related to physical security. Should such a need arise, such as an emergency that requires briefing the Commission on an event captured in an Annual Report, the ITPs could serve as a means of conferencing that would provide the information the Commission requires and that the utilities wish to closely safeguard.

Provisions for Remote Live Conferencing

The IOUs shall make available a secure teleconferencing platform for the purpose of facilitating remote briefings when travel and/ or face-to-face interactions are impracticable due to emergencies or public health orders. The secure teleconferencing platform would allow for both a slide presentation and a “face-to-face” capability to view speakers/ participants. An additional platform component would allow CPUC staff in real-time access to searchable electronic copies of confidential physical security documents in unredacted format.

² OP 29: “Utilities shall provide to the Director of the Safety and Enforcement Division and Energy Division copies of OE-417 reports submitted to the United States Department of Energy (U.S. DOE) within two weeks of filing with U.S. DOE.”

The IOUs shall adopt a single statewide virtual platform via portable computer that offers turnkey ease of use with minimal log-in hassle, and that serves as an all-in-one tool for secure data access such that it accommodates real-time data transfer and face-to-face teleconferencing without the need to suppress or redact presentation materials. Such a laptop or tablet device, provided to CPUC staff reviewers on an as-needed basis, would be internet compatible to allow for real-time remote access to data and updates to regulatory filings, and for the purpose of ensuring virtual platform functionality, including an ability for remote access by IOU staff.

The IOUs are instructed to collaborate to devise a single virtual platform and data facilitation software package to be loaded onto a common portable computing device such that each designated Commission staff reviewer, upon request and upon physical security IOU work product assignment, shall be assigned one universal device having consistent user experience and log in protocol, to be provided by the joint electric IOUs for statewide regulatory purposes.

The universal statewide computer platform shall be delivered (i) fully charged; with (ii) full troubleshooting measures taken to ensure that all software operates as intended (subject to automated software updates to assure system security and reliability); and (iii) in good operating and clean condition; with (iv) return prepaid return shipping label to each assigned CPUC staff reviewer; by (v) secure tracked parcel shipping; (vi) no less than two weeks prior to the work product due date. SPD staff shall reserve the right to an orientation tutorial with IOU staff for the purpose of instruction on the unique operational features of the remote virtual platform to be held no less than one week prior to the work product due date.

An exception to the requirements for the universal portable computer platform shall be available by means of a secure FTP (File Transfer Protocol) or VDI (Virtual Desktop Infrastructure) (collectively “alternative virtual platforms” or “AVPs”), so long as the AVPs, alone or in tandem with another existing commonly-accepted secure video streaming technology (such as Cisco Webex) can facilitate both viewing of IOU work products by Commission staff and remote teleconferencing with a level of security such that suppression or redaction of presentation materials shall be unnecessary. Under no circumstance shall the AVPs enable permanent transfer of IOU information to a Commission-owned computer such that Commission staff would be rendered custody of physical security data deemed sensitive.

Such a proxy substitute remote platform would be activated at the direction of CPUC staff, and by consent of CPUC staff should IOU staff request such accommodation.

The requirements as prescribed within the ITPs, both within *Provisions for Remote Live Conferencing* and the *Five-step Process* shall apply fully to virtual meetings. Should IOU staff require any exception to the rules and procedures, the applicable IOU lead staff shall provide a written request for an exception to the lead SPD staff no less than one week prior to the IOU’s scheduled briefing date, explaining the issue and hardship, if any, and the IOU’s proposed relief.

Utilities pursuing a cooperative agreement to put forward a universal portable virtual platform shall not be prejudiced by other utilities’ non-participation in the effort.

Provisions to Establish Interim Trial Procedures as Permanent Procedures

Factors to Determine Effectiveness of Interim Trial Procedures

Key questions that may be considered and addressed in judging ITPs reversion to permanent status include:

- Do ITPs provide Commission staff with adequate information necessary to duly carry out Physical Security regulations while ensuring the safeguarding of sensitive data?
- Are Commission and IOU staff satisfied with the ITPs and find them to provide adequate value?
- Are better alternatives available?

Five-step Process of Interim Trial Procedures

Step 1. Scheduling IOU-CPUC briefing. No less than three weeks prior to the due date for a physical security work product due to the CPUC, IOU staff shall email assigned SPD staff with an alert containing a request for an in-person meeting with assigned SPD staff for the purpose of holding a confidential briefing and proposing potential meeting dates. The email alert shall advise SPD of each IOU's lead staff assigned to the project. This meeting may be scheduled prior to and up to two weeks after the due date of the work product. The IOUs shall coordinate among themselves and with SPD to schedule the briefings more or less evenly across the weeks allocated. Step 1 requirements may be addressed jointly by the IOUs, so long as they have clearly identified a lead liaison to SPD to carry out the effort.

Step 2. Briefing Planning Coordination with CPUC Staff. SPD will locate suitable meeting space at the Commission and determine staff to attend. After, SPD will confirm a time and date.

Step 3. Required Work Product Submittal. IOU staff shall provide CPUC staff with electronic, searchable, redacted versions of the work product on or before the due date, and with printed unredacted copies hand-delivered at the Presentation Meeting.

Step 4. Presentation Meeting. The closed-door confidential briefing shall have an individual IOU's team explain the full extent and contents of the relevant required physical security work product, which should include presentation visuals (if electronic, fully supported by IOU hardware (e.g., projector, screen, cables, etc.) and hard copies of any reports. In addition, IOU staff shall, at the briefing meeting, provide one laptop computer with power cord for exclusive use by each participating CPUC staff and which shall contain an unredacted, electronic, searchable version of the relevant work product. To satisfy the laptop requirement, utilities may make available the portable virtual platform described within *Provisions for Remote Live Conferencing*.

Provided IOU unredacted work products shall be maintained within view of IOU staff during CPUC staff review. Should CPUC staff, in the course of the briefing meeting and work product review, find it necessary to confer privately, the CPUC staff shall locate alternative meeting space outside the location of the briefing.

At the conclusion of the briefing, IOU staff shall retain original sensitive information documentation (including any unredacted reports), and CPUC staff will retain any notes taken.

Step 5. Recording of IOU Compliance in OP Enforcement Tracking Log. Upon successful fulfillment of Steps 1 through 4, SPD will indicate in the Commission's internal database that each applicable IOU is in compliance with the applicable OP within D.19-01-018. SPD shall provide notice of such to each IOU as applicable.