SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

Michael A. Backstrom
VP Regulatory Policy
Michael.backstrom@sce.com

07/30/2021

Caroline Thomas Jacobs, Director
Office of Energy Infrastructure Safety
300 Capitol Mall, Suite 500
Sacramento, CA 95814
info@energysafety.ca.gov

BY OEIS E-FILING

Reference Attorney
Office of Administrative Law
300 Capitol Mall, Suite 1250
Sacramento, CA 95814
staff@oal.ca.gov

SUBJECT: Office of Administrative Law File Number 2021-0726-01E

Southern California Edison Company's Comments on Proposed Emergency Process and Procedure Regulations Submitted with Proposed Emergency Rulemaking Action by the Office of Energy Infrastructure Safety to the Office of Administrative Law on July 13, 2021.

Dear Director Thomas Jacobs and Office of Administrative Law Reference Attorney:

Pursuant to California Government Code Section 11349.6(b) and 1 California Code of Regulations Section 55, Southern California Edison Company (SCE) hereby submits its comments on the Proposed Emergency Process and Procedure Regulations Noticed with the Proposed Emergency Rulemaking Action by the Office of Energy Infrastructure Safety (Energy Safety) to the Office of Administrative Law (OAL) on July 26, 2021. SCE appreciates the opportunity to provide these comments, which generally support the proposed regulations, with particular exceptions discussed below.

INTRODUCTION

SCE agrees that "[i]n order for the Energy Safety to be ready to perform its vital work as a new office within CNRA shortly after July 1, 2021, Energy Safety will need regulations that establish a process and procedures, effective immediately, that will form the

structure of its operations in meeting its statutory mandates."[1] Energy Safety is a newly formed agency established under Government Code Sections 15470, *et seq*. As Energy Safety points out, "[t]he Energy Safety is the successor to, and, effective July 1, 2021, is vested with, all of the duties, powers, and responsibilities of the Wildfire Safety Division established pursuant to Public Utilities Code section 326, including, but not limited to, the power to compel information and conduct investigations."[2] For the most part, SCE supports the regulations Energy Safety proposes as the successor to WSD. That said, several proposed regulations create issues that would largely be resolved by continuing with existing California Public Utilities Commission (CPUC or Commission) requirements that have generally functioned well and are familiar to stakeholders rather than shifting to other regulatory models, e.g., State Energy Resources Conservation and Development Commission's (California Energy Commission) model regarding confidentiality designation, or developing new regulations that could cause confusion, unnecessary burden, duplication of effort, and potential jurisdictional issues.

Where indicated, the CPUC has in place reasonable, equally effective alternatives to the more burdensome regulations proposed by Energy Safety, but Energy Safety has not described these alternatives or explained why it has rejected them.[3] In such cases, the CPUC alternatives are established means of achieving substantially the same apparent objectives[4] as the proposed regulations, and the CPUC alternatives are relatively clear and familiar to stakeholders.

In particular, SCE recommends modifications and/or clarifications to the Proposed Regulations below. Where noted, the Proposed Regulations as written appear to be in conflict with one or more of the California Administrative Procedure Act (APA)[5] standards, e.g., inconsistent with statute (Government Code Section 11342.2); unclear (Government Code Section 11349(c)); duplicative; and/or unnecessary.

- Section 29200: Confidential Information
- Section 29201: Disclosure of Confidential Information
- Section 29300: Notification

---

[1] Energy Safety Adoption of Emergency Rulemaking Action Process and Procedure Regulations, Notice of Proposed Emergency Action (Notice), p. 3.

[2] OEIS Adoption of Emergency Rulemaking Action Process and Procedure Regulations, Notice of Proposed Emergency Action (Notice), p. 3.

[3] "Every agency subject to this chapter shall prepare, submit to the [Office of Administrative Law] with the notice of the proposed action as described in Section 11346.5, and make available to the public upon request, all of the following:...An initial statement of reasons for proposing the adoption, amendment, or repeal of a regulation. This statement shall include, but not be limited to, all of the following: *A description of reasonable alternatives to the regulation and the agency's reasons for rejecting those alternatives. Reasonable alternatives to be considered include*, but are not limited to, *alternatives that are proposed as less burdensome and equally effective in achieving the purposes of the regulation* in a manner that ensures full compliance with the authorizing statute or other law being implemented or made specific by the proposed regulation." Government Code Section 11346.2(b)(4)(A).

[4] As noted below, however, the objective is not always clear based on the proposed regulations as written.

[5] Government Code Section 11340, *et seq.*

- Section 29301: Incident Report
- Section 29302: Investigations, Notices of Defects and Violations and Referral to the Commission

COMMENTS ON NOTICE AND PROPOSED REGULATIONS

1. Section 29200 Should Be Modified to Adopt CPUC Requirements Currently Used for Confidentiality Designations

Energy Safety notes that the language of Section 29200 "is modeled from other agency regulatory language previously approved by OAL," and cites California Code of Regulations, Title 20, section 2505.[6] With some omissions, additions and modifications, Section 29200 generally follows 20 CCR Section 2505, "Designation of Confidential Records," the regulation used by the California Energy Commission.

As a general matter, SCE proposes that the Energy Safety continue to use the confidentiality designation requirements developed by the CPUC in CPUC Decisions 06-06-066 (energy procurement); 16-08-024;17-09-023; and General Order 66-D. These confidentiality designation requirements were developed over a series of rulemakings and reflect a considerable amount of stakeholder input and public process. Further, the CPUC's confidentiality declaration/matrix process is familiar to stakeholders in the context of the WMP and appears to have functioned well thus far through successive WMP processes. Given the potentially devastating consequences associated with inadvertent disclosure of sensitive information such as critical energy infrastructure information (CEII), it would be prudent to continue with a proven confidentiality designation process familiar to WMP stakeholders, especially in the context of a high volume of data requests with a relatively short response period. The requirement for Deputy Director (and possibly Director) review for every confidentiality request exacerbates these issues. Finally, it is unnecessarily burdensome to require two distinct processes for providing confidential material to the CPUC and Energy Safety.

In addition to this general concern, SCE raises the following specific issues with respect to Proposed Regulation Section 29200.

Section 29200(a)(6), a provision not included either in 20 CCR Section 2505 or the CPUC's confidentiality designation requirements, requires specific information in support of a confidentiality designation for CEII, including "whether the information would allow a bad actor to attack, compromise or incapacitate physically or electronically a facility providing critical utility service" and "whether the information discusses vulnerabilities of a facility providing critical utility service."[7] This level of detail

[6] Notice, p. 10.

[7] "If the applicant believes that the record should not be disclosed because it contains critical energy infrastructure information, the application shall also state: (A) whether the information is customarily in the

is not required in the confidentiality designation and matrix/declaration processes under CPUC Decisions 06-06-066 (energy procurement); 16-08-024;17-09-023; and General Order 66-D. The information in this proposed regulation highlights how a bad actor could abuse the CEII, undermining the very purpose of a confidentiality process. SCE recommends this provision be removed from the regulation. Instead, SCE recommends that Energy Safety follow up with the information provider in a confidential communication if there are questions regarding the basis for particular confidentiality designation requests.[8]

Section 29200(a)(6),[9] which concerns aggregated information, is another provision not contained either in 20 CCR Section 2505 or the CPUC's confidentiality requirements. It requires that the application "state whether the information may be disclosed if it is aggregated with other information or masked to conceal certain portions, and if so the degree of aggregation or masking required. If the information cannot be disclosed even if aggregated or masked, the application shall justify why it cannot." SCE is not certain what this draft regulation is intended to accomplish. It could be intended to require that applicants explain why aggregation or masking of data is not an option because there is no way to aggregate or mask the data to make it non-confidential. Or it could be intended to provide confidentiality protection for information that, while in itself may not be confidential, in aggregate with other information raises confidentiality issues, e.g., separate documents with asset data that when read together show the criticality of the asset and potential impacts to the system if that asset were to be disabled. Both are sound objectives but as written the intent is unclear. SCE recommends that this provision be clarified accordingly.

Section 29200(b) provides "A deficient or incomplete application shall be returned to the applicant with a statement of its defects and a request for additional information. If the missing information, or a request for an extension of time to respond, is not submitted within fourteen days of receipt of the request, the Deputy Director may deny the

---

public domain such as the location of visible equipment; (B) whether the information would allow a bad actor to attack, compromise or incapacitate physically or electronically a facility providing critical utility service; (C) whether the information discusses vulnerabilities of a facility providing critical utility service; (D) whether the information has been voluntarily submitted to the Office of Emergency services as set forth in Government Code section 6254(ab); (E) whether the information or substantially similar information was classified as protected critical infrastructure information by the Department of Homeland Security or Department of Energy." Section 29200(a)(6), Proposed Regulations, p. 5.

[8] Section 29200(a)(5) (emphasis added), apparently modeled after 20 CCR Section 2505(a)(1)(D), raises similar concerns: "If the applicant believes that the record should not be disclosed because it contains trade secrets or its disclosure would otherwise cause loss of a competitive advantage, *the application shall also state the specific nature of that advantage and how it would be lost, including the value of the information to the applicant, and the ease or difficulty with which the information could be legitimately acquired or duplicated by others*." Here, too, it is not prudent to require this level of explicit detail, at least in the initial application.

[9] "[S]tate whether the information may be disclosed if it is aggregated with other information or masked to conceal certain portions, and if so the degree of aggregation or masking required. If the information cannot be disclosed even if aggregated or masked, the application shall justify why it cannot;" Section 29200(a)(7), Proposed Regulations, p. 6.

application."[10] This proposed regulation is a modification of 20 CCR Section 2505(a)(2),[11] which does not specifically state an application shall be denied if conditions are not met within the fourteen day period. The CPUC does not include such a provision. To avoid disclosure of confidential information in the event that the applicant does not receive timely notice from the Energy Safety or due to some other miscommunication, SCE requests that this proposed regulation be modified to require that the Deputy Director confirm receipt by the applicant of the returned application.

The Proposed Regulations do not include 20 CCR Section 2505(a)(6), which provides as follows: "Failure to request confidentiality at the time a record is submitted to the Commission does not waive the right to request confidentiality later; however, once a record has been released to the public, the record can no longer be deemed confidential. Although a record designated as confidential shall remain confidential during the application and appeal process, subject to the provisions of Section 2507(b) of this Article, the application itself is a public document and can be released."[12] Notwithstanding whether the OEIS adopts the CPUC confidentiality designation approach, SCE proposes that this provision be adopted so that an applicant may preserve the right to designate material confidential prior to public disclosure.

a. The Regulations Should Provide for a "Closed Room" Approach to Temporarily Share "Security Sensitive" Confidential Information

In most instances, SCE anticipates providing sensitive utility information directly to Energy Safety, as envisioned in the preceding proposed regulations. For example, in the vast majority of instances that CPUC has sought SCE data, including sensitive data, SCE has provided it directly to CPUC. SCE anticipates doing the same with Energy Safety.

However, as security risks to electric infrastructure grow and evolve, so should methods of sharing highly sensitive information between regulatory agencies and those being regulated. Based on new and emerging threats, SCE respectfully urges Energy Safety to recognize a new class of data – "Security Sensitive Information" – information about a regulated utility's infrastructure, operations or security defenses, that is so sensitive that it merits use of special handling and sharing processes, even for Energy Safety regulatory review. Such information may include, *but is not limited to*, information (i) relating to SCE's critical infrastructure, (ii) physical security, and (iii) cybersecurity.

Specifically, instead of requiring regulated entities to turn over Security Sensitive information directly to Energy Safety, SCE urges Energy Safety to view "Security Sensitive Information" on a temporary basis using a "closed room" approach – whether

---

[10] Section 29200(b), Proposed Regulations, p. 6.

[11] "A deficient or incomplete application shall be returned to the applicant with a statement of its defects. The record or records for which confidentiality was requested shall not be disclosed for fourteen days after return of the application to allow a new application to be submitted except as provided in Section 2507 of this Article." 20 CCR Section 2505(a)(2).

[12] 20 CCR Section 2505(a)(6).

physical or virtual. For example, should Energy Safety request viewing hard-copy versions of Security Sensitive information, SCE and Energy Safety would meet at a mutually convenient location. SCE would provide the data to Energy Safety for review during a closed-room session. Upon completing that review, the information is returned to SCE. Alternatively, should Energy Safety wish to view this information electronically, then SCE would make this information available to Energy Safety for remote viewing. Although accessible from Energy Safety computers, the information would not leave SCE's systems and repositories. The same process would apply for other regulated utilities providing "Security Sensitive Information" to Energy Safety.

The security risks triggering SCE's proposal are real, raising issues of not only informational security but also of US national security. As regulatory agencies accumulate greater information about regulated entities, they become more attractive targets to adversarial, sophisticated threat actors with the resources of entire countries behind them. For example, malicious foreign nationals associated with the Republican Guard of the Nation of Iran have successfully penetrated the Federal Energy Regulatory Commission (FERC) – an attack that then-United States Attorney Geoffrey Berman considered especially concerning because FERC holds details of some of the country's most sensitive infrastructure."[13] And the recent, highly publicized "SolarWinds" attack, shows that government agencies remain squarely within the crosshairs of malicious adversaries seeking to steal their secrets.[14] This represents but the tip of the iceberg in terms of national security threats facing government and regulatory agencies.[15]

In order to proactively mitigate against this regulatory targeting, electric utility regulators have already started authorizing use of temporary, closed door, regulatory review of a utility's most sensitive data. For example, at the federal level, the North American Electric Reliability Corporation (NERC) faced this same issue in promulgating Critical Infrastructure Protection ("CIP") Standard No. CIP-014-1 (Physical Security).[16] NERC promulgated this regulatory standard in response to the highly publicized "Metcalf Substation" shooting, where unknown assailants used high-powered rifles to incapacitate a California electric substation.[17] CIP-014-1 requires utilities to create highly sensitive information, such as locations of priority facilities; vulnerability

---

[13] Dustin Voltz, U.S. charges, sanctions Iranians for global cyber attacks on behalf of Tehran, Reuters (March 23, 2018), at https://www.reuters.com/article/us-usa-cyber-iran/u-s-charges-sanctions-iranians-for-global-cyber-attacks-on-behalf-of-tehran-idUSKBN1GZ22K

[14] Bill Whittaker, SolarWinds: How Russian Spies Hacked the Justice, State, Treasury, Energy and Commerce Departments (July 4, 2021), at https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-07-04/.

[15] For more information about this issue, *see* Resubmission of Petition for Modification of Decision 19-01-018, CPUC Rulemaking No. R.15-06-009 (Jan. 16, 2020), at https://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M324/K944/324944685.PDF

[16] NERC CIP Standard CIP-014-01, at C.1.4, available at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-1.pdf.

[17] Phase I Decision on Order Instituting Rulemaking Regarding the Physical Security of Electrical Corporations, Decision D.19-01-018 (Jan. 22, 2019), at pp.3-4, at https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M260/K335/260335905.docx

assessment; and mitigation plans.[18] The standard also requires utilities to share that information with NERC for regulatory audit.[19]

However, CIP-014-1 does NOT require utilities to send security-sensitive information directly to NERC for regulatory review. Instead, this standard specifically mandates that that such data should not leave the utility's environment.[20] Instead, regulated utilities provide this information temporarily to NERC for regulatory review. Since then, NERC expanded use of closed room sharing methods by permitting utilities to create virtual "Secure Evidence Lockers" to be located within each utility's online systems.[21] Once implemented, NERC may use these secure evidence lockers to remotely view a regulated utility's highly sensitive cybersecurity information, without that information leaving that utility's systems.

In California, the Commission's Safety and Enforcement Division (SED) authorized utilities regulated by the Commission to share highly sensitive physical security-related information with SED analysts in 2020 and 2021 using virtual sharing methods such as the ones proposed in these comments.[22]

For the above reasons, SCE respectfully urges Energy Safety to adopt regulations permitting use of closed room procedures – whether virtual or physical – to view a utility's most "Security Sensitive" data without that data leaving the utility's custody.

2. Section 29201 Should Be Clarified to Require Formal Agreements to Keep Material Confidential and Notice to Designating Entities in All Cases of Interagency Disclosure

Section 29201, "Disclosure of Confidential Information", includes provisions allowing conditions under which Energy Safety "may disclose confidential information received by the Office from outside entities or persons."[23] Energy Safety notes that the language of Section 29201 "is modeled from other agency regulatory language previously approved by OAL," and cites California Code of Regulations, Title 20, section 2507.[24] Under Section 2901, Energy Safety can disclose confidential material to certain of those

---

[18] *Id., supra* n.14, at Section B (identifying risk assessment and mitigation process).
[19] *Id.*at Section C.1.4 (identifying information security requirements).
[20] *Id.*
[21] NERC, Registered Entity Maintained Secure Evidence Lockers – Functional Specification v.9, at p.1 (Jan. 298, 2021), available at https://www.nerc.com/ResourceCenter/Align%20Documents/1-Align%20Registered%20Entity%20SEL%20Functional%20Requirements%20February%202021.pdf
[22] Letter from Dan Bout, Director of Safety Policy Division, to Parties to Physical Security Proceeding, CPUC Proceeding No. R.15-06-009, dated Dec. 4, 2020 (authorizing regulated utilities to share physical security data with CPUC using virtual sharing platforms). This letter, and earlier versions, at https://www.cpuc.ca.gov/about-cpuc/divisions/safety-policy-division/risk-assessment-and-safety-analytics/physical-security-of-electric-infrastructure
[23] Section 29201(a), Proposed Regulations, p. 7.
[24] Notice, p. 10.

persons that work for Energy Safety (Section 29201(a)(1) and (2)), as well as other governmental agencies (Section 29201(a)(3) and (4)). However, while 29201(a)(3) specifically requires "government bodies" "agree to keep the records confidential", subpart (4) does not explicitly require the same of the specific agencies named, i.e., the California Department of Forestry and Fire Protection, California Energy Commission, and the California Public Utilities Commission.[25] SCE requests that the Regulations specify that those named agencies be required to agree to keep the material confidential, as is required in the previous subsection. SCE also requests that the regulation be modified to require that confidential information providers be given notice of any interagency sharing of that provider's confidential information. Finally, SCE requests that as a policy matter such interagency sharing of confidential information be limited as much as reasonably possible because as a practical matter, the more widely information is distributed the more likely the confidential material will be inadvertently disclosed, at great potential risk to the public.

3. The Scope of Issues Requiring Notification Under Section 29300 Should Be Clarified

Section 29300, "Notification", in its entirety, reads "The Director, or designee, shall be notified within 24 hours from the time an electrical corporation becomes aware of a wildfire threat to electrical infrastructure it owns or operates. The Director, or designee, shall be notified within 24 hours from the time a regulated entity becomes aware of infrastructure that it owns or operates being investigated for involvement in potentially causing an ignition."[26] As written, this draft regulation is vague and potentially overbroad and unduly burdensome. For example, "wildfire threat" could mean any number of minor issues for which a 24-hour notification requirement would be overbroad and unreasonably burdensome. Under this language, "wildfire threat" could be construed to include a relatively small ignition next to a pole creating a reliability issue, but no significant wildfire threat. Reporting every such "wildfire threat" to any electrical asset within 24 hours would require an enormous amount of time and effort and unnecessarily divert resources.

---

[25] "(a) The Director may disclose confidential information received by the Office from outside entities or persons to: (1) Office employees or representatives whose work requires inspection of the information; (2) Contractors and consultants to the Office whose work for the Office requires inspection of the information and who agree in a contract or separate non-disclosure agreement to keep the records confidential; and (3) Other governmental bodies that need the records to perform their official functions and that agree to keep the records confidential and to disclose the records only to those employees or contractors whose agency work requires inspection of the records. (4) Under Public Utilities Code section 8386.5, Public Resources Code sections 25216.5 and 25224, and Title 20, California Code of Regulations section 2505(b), confidential information in the custody or control of the Office may be shared with the California Department of Forestry and Fire Protection, California Energy Commission, and California Public Utilities Commission. Upon receipt of a request for data from those agencies, confidential information may be shared without the need for an interagency agreement." Section 29201(a), Proposed Regulations, p. 7.

[26] Section 29300, Proposed Regulations, p. 8.

Further, this provision does not clarify what type of “investigation" or by what agency or agencies would qualify. Thus, this Proposed Regulation is unclear under the APA.[27] Rather than reinvent the proverbial wheel, to avoid confusion and inefficiency associated with duplication of effort, SCE recommends that the regulation be revised to state that SCE shall provide the same information, and under the same circumstances, as in the established Electric Safety Incident Report (ESIR) used at the CPUC. The ESIR is a report required by the CPUC if SCE’s facilities are involved in certain types of events: (1) a fatality or serious injury involving electric facilities; (2) damage to property of the utility or others in excess of $50,000; (3) significant media coverage, and is submitted within 2 hours during business hours or within 4 hours outside of business hours.[28] The ESIR provides more specificity regarding content, triggers, and timing than this Proposed Regulation and would appear to cover the same content sought by Energy Safety through this proposed regulation. Alternatively, SCE recommends stakeholder discussions or workshops to clarify what Energy Safety attempts to cover by this provision.

4. The Scope of Reporting Under Section 29301 Should Be Clarified

Section 29301, “Incident Report”, directs regulated entities to submit an incident report within 30 days containing, among other information, factual or physical evidence related to the incident, contact information of any known witnesses, preliminary root cause analysis, and description of all actions taken to minimize recurrence.[29] This provision raises several concerns. First, in subpart (b)(3), “*preliminary* root cause” analysis is a vague term that requires clarification—“root cause” investigations have a particular meaning, completion of which often requires more than 30 days in the experience of SCE. The reference to “detailed discussion of *all* findings” in that subpart (emphasis added) raises issues concerning information protected by the attorney-client privilege and attorney work product doctrine. Second, the requirement in subpart (b)(4) to describe “all actions taken, if any, to minimize the recurrence of such incidents” within 30 days is an insufficient amount of time because in SCE’s experience it typically takes more time to identify appropriate mitigation measures. Third, subpart (b)(7) is vague and could be burdensome to provide within 30 days depending on what “any other information” is intended to include. Thus, this Proposed Regulation is unclear and unnecessary under the APA.[30] Similar to SCE’s comments regarding Proposed Regulation 29300, above, SCE recommends that Proposed Regulation 29301 be revised to require the same information SCE currently provides to the CPUC under its

[27] Government Code Section 11340, *et seq.*
[28] Example of ESIR @ https://www.edison.com/content/dam/eix/documents/investors/wildfires-document-library/esir-20201207-201207-13722.pdf
[29] Section 29301, Proposed Regulations, p. 8.
[30] Government Code Section 11340, *et seq.*

well-established process pursuant to Public Utilities Code Section 315.[31] Such information includes the underlying facts of the fire as known by SCE at the time of reporting. Additionally, any proposed regulation requiring submission of incident reports should include a provision to the same effect as PUC Section 315, which provides: "Neither the order or recommendation of the commission nor any accident report filed with the commission shall be admitted as evidence in any action for damages based on or arising out of such loss of life, or injury to person or property."

5. The Scope of Inspections Under Section 29302 Should Be Clarified

Section 29302, "Investigations, Notices of Defects and Violations and Referral to the Commission", would allow Energy Safety to designate investigators to, for example, investigate whether an approved WMP was followed or if failure to do so contributed to the cause of a wildfire (or conduct other investigations). This provision also would allow Energy Safety to designate a compliance officer to consider the findings of any investigation and specifies how notices of violation will be served. Finally, the provision would allow Energy Safety to recommend to the Commission that it pursue enforcement action in the event of noncompliance with an approved WMP plan.[32]

Similar to SCE's comments regarding Proposed Regulations 29300 and 29301, above, SCE recommends that Proposed Regulation 29302 be revised to require the same information SCE currently provides to the CPUC under its well-established process pursuant to Public Utilities Code Section 315. Such information includes the underlying facts of the fire as known by SCE at the time of reporting. Creating a different set of requirements through this Proposed Regulation will likely result in duplicative processes—simultaneous investigations into the same incidents by OEIS and the CPUC—and the potential for inconsistent rulings and findings. As with Section 315, SCE asks that the following safeguards also be implemented, "Neither the order or recommendation of the commission nor any accident report filed with the commission shall be admitted as evidence in any action for damages based on or arising out of such loss of life, or injury to person or property."

Further, it is not clear that Energy Safety has the jurisdictional authority to conduct the investigations described as drafted, particularly in a(3) and a(4). These provisions state that "The Director may designate investigators to investigate the following: (3) *Whether the regulated entity is noncompliant with its duties and responsibilities* or has otherwise committed violations of any laws, regulations, or guidelines within the authority of the Office; and (4) *Other related investigations* by the Director." The italicized language (added here for emphasis) as written potentially exceeds the Energy Safety's jurisdictional authority as codified in Public Utilities Code Section 326 and Government

[31] Public Utilities Code Section 315; Example of Section 315 letter @https://www.edison.com/content/dam/eix/documents/investors/wildfires-document-library/section-315-20210104-202014197.pdf

[32] Section 29302, Proposed Regulations, p. 9.

Code Section 15475, et seq. Any "investigation" under this Proposed Regulation must be explicitly limited to wildfire safety, or it is potentially invalid under Government Code Section 11342.2.[33]

CONCLUSION

SCE appreciates the opportunity to submit its comments on Energy Safety's Notice and Proposed Regulations.

Sincerely,

//s//

Michael A. Backstrom
VP Regulatory Policy
Southern California Edison

cc: Service List for R.18-10-007
info@energysafety.ca.gov
staff@oal.ca.gov
nathan.poon@energysafety.ca.gov

[33] "Whenever by the express or implied terms of any statute a state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, no regulation adopted is valid or effective unless consistent and not in conflict with the statute and reasonably necessary to effectuate the purpose of the statute." Government Code Section 11342.2.