

**BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA**

Order Instituting Rulemaking to Continue
Implementation and Administration of the California
Renewables Portfolio Standard Program.

Rulemaking 08-08-009
(Filed August 21, 2008)

**DECLARATION OF WILLIAM C. SAUNTRY ON BEHALF OF SAN DIEGO GAS &
ELECTRIC COMPANY (U 902 E) IN SUPPORT OF JOINT PETITION FOR
MODIFICATION**

I, William C. Sauntry, do hereby declare:

1. I am the Risk and Compliance Manager within Corporate Security for Sempra Energy, of which San Diego Gas & Electric Company (“SDG&E”) is a subsidiary. I make this Declaration on behalf of SDG&E in support of the Joint Petition for Modification submitted on behalf of Pacific Gas and Electric Company, Southern California Edison Company, and SDG&E. I have personal knowledge of the matters referred to herein and, if called upon to testify, I could and would competently testify thereto.

2. In my current role, I am responsible for the implementation of a risk management and intelligence program to prioritize and mitigate threats, vulnerabilities, and consequences to the company and its infrastructure. Before this role, I was the supervisor for the Critical Infrastructure Protection, Cyber Intelligence, and the Geospatial Intelligence Units within the San Diego Law Enforcement Coordination Center, a Department of Homeland Security (“DHS”) fusion center, which is part of the California State Threat Assessment System. In that role, I performed vulnerability assessments for the California Office of Emergency Services and the

County of San Diego to evaluate the security of critical infrastructure. I have also worked for DHS performing vulnerability assessments on infrastructure throughout the nation. The first step in each of these assessments was to review online material for sensitive information, which may be used to plan attacks against infrastructure. In addition, I understand the breadth of information included within Geographic Information System (“GIS”) data and how important it can be to assist with pre-operational planning of attacks on critical infrastructure.

3. SDG&E takes protective measures to minimize the potential of critical information being used to attack and disrupt California’s electric system. This information may be used in preoperational planning of attacks by malicious actors, allowing them to plan an attack remotely, without having seen or been present at any of the facilities.
4. SDG&E treats its GIS data with special care because it recognizes that precise critical infrastructure information that is made publicly available—for instance, through publication of otherwise non-public GIS data—may be misused. For example, the public availability of this information may limit or eliminate the need for a malicious actor to perform onsite reconnaissance or surveillance to assist with target selection. This enhances preoperational planning of an attack because it reduces the chances that a malicious actor will be detected and/or apprehended in the early stages of an attack. Stopping an attack during preoperational planning is preferred to responding to an attack while in progress. Identifying potential indicators of an attack, such as onsite reconnaissance or surveillance, is such an important component of preventing terrorism, DHS has created a national

campaign called “If you see something, say something,”¹ to recognize and report suspicious activity. This campaign is part of the National Suspicious Activity Reporting (“SAR”) Initiative (“NSI”). Recent research on the Nationwide SAR Initiative, an effort to establish reporting standards with respect to SARS, has validated that there is good alignment between pre-incident activities of previous terrorist attacks and the indicators identified as important by the NSI.

5. Furthermore, this research has found that some of these indicators were observable by the public prior to an attack.² Additionally, the RAND Homeland Security and Defense Center report titled, “Terrorist Plots Against the United State, what We Have Really Faced, and How We Might Best Defense Against It” (September 2015), states between 1995 to 2012, SARs constituted the third largest source of initial clues leading to foiling plots. A wide variation of types of suspicious activity reported, including potential target site surveillance.³
6. Electric transmission and distribution system facility information, such as location and configuration (*e.g.*, identification, routing, ratings, loading, status), are especially sensitive because this information provides a holistic system overview as well as detailed information that may assist with the identification of a single point of failure, choke points, or nodes servicing critical infrastructure. Maps and configuration of the electric system may allow a malicious actor to more easily

¹ Department of Homeland Security, “If You See Something, Say Something,” *available at* <https://www.dhs.gov/see-something-say-something>.

² University of Maryland, Study of Terrorism and Responses to Terrorism, “Research Brief: Validation of the Nationwide Suspicious Activity Reporting (SAR) Initiative” (2015), *available at* https://www.start.umd.edu/pubs/STARTResearchBrief_NationalSARInitiative_March2015.pdf.

³ RAND Homeland Security and Defense Center, “Terrorist Plots Against the United State, What We Have Really Faced, and How We Might Best Defense Against It” (September 2015) at 11, *available at* https://www.rand.org/content/dam/rand/pubs/working_papers/WR1100/WR1113/RAND_WR1113.pdf.

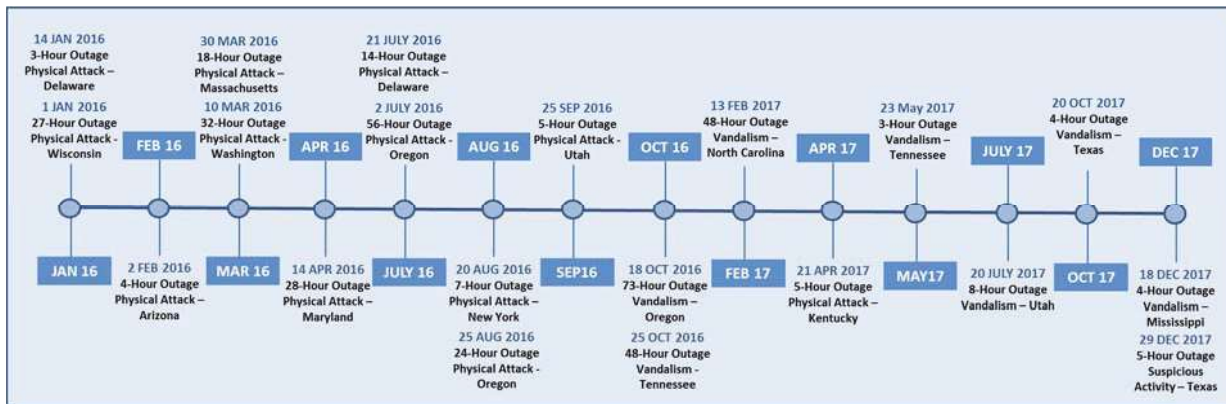
identify the location of infrastructure necessary to disrupt electric service to life/safety, national defense, communications, or other critical infrastructure.

7. Remote planners can use detailed information and locations to evaluate the electric system and security locations and vulnerabilities at point along electric system; this of course can be accomplished from afar without any risk of detection by law enforcement or company personnel.
8. Even assuming that a bad actor could theoretically obtain the similar information that is in the online access portal from other means, such as onsite reconnaissance (which they cannot), or data sources the increased availability (e.g., more sources) and granularity of publicly accessible safety- and security-sensitive data would accelerate target selection and maximize the consequences of an attack. Having ready and on-going access to increased amounts of this type of data allows the malicious actor to complete the targeting phase of the attack remotely and more expeditiously because the detailed and time-intensive planning steps discussed above would be unnecessary.
9. Therefore, although the Commission has ordered public access to some maps and information of the electric system in the past, SDG&E has an even better understanding of the threats against electric infrastructure through the hiring of risk and intelligence analysts to provide threat analysis. If this data were misused and electric infrastructure were disrupted or attacked, critical infrastructure within San Diego region may be affected, with a real risk of harm to life and property.
10. The risk of third-party action, whether acts of terrorism, theft, or vandalism, is not speculative. Utilities are mandated by the Department of Energy, Office of

Electricity Delivery and Energy Reliability (“OE”) to report the causes of major interruptions or outages through the Electric Emergency Incident and Disturbance Report (OE-417). The following table provides OE-417 statistics of incidents caused by actual or suspected physical attacks, sabotage, and vandalism:

	2014	2015	2016	2017
Total Reports	73	42	44	44
WECC Region	31	23	26	23

The following illustration lists the incidents with restoration greater than three hours between January 2016 and December 2017.



11. Several other incidents have highlighted malicious intent against the electric system including:

- In April 2013, the Metcalf transmission substation in San Jose, California, was attacked by gunfire resulting in damaging of 17 transformers, 6 circuit breakers, and release of 52,000 gallons of oil. As part of the attack, AT&T and Level 3 fiber optic communication cables were severed.⁴
- In September 2016, Stephen McRae reportedly shot at a Garkane Energy

⁴ California Public Utilities Commission, “PG&E Metcalf Incident and Substation Security,” available at http://www.cpuc.ca.gov/uploadedFiles/CPUC_Website/Content/Safety/Presentations_for_Commission_Meeting/SafetySlidesfromPowerPointforthe22714Meeting3331.pdf.

Cooperative substation, damaging a transformer and causing a power outage of around 13,000 people in Kane and Garfield counties. This is an open case with pending charges of ‘Destruction of an Energy Facility,’ ‘Unlawful Possession of a Firearm,’ and ‘Possession of Marijuana.’⁵

- In December 2014, a pilot and owner of a flight school reportedly threw objects on Hydro Quebec’s high voltage power lines affecting over 188,000 households in Quebec, Canada. This is currently an open case and involves a \$28.6M lawsuit.⁶
- Three separate incidents occurred in Arkansas from August 2013 until October 2013. Investigators successfully linked these incidents and arrested one individual, Jason Woodring, on charges of destruction of an energy facility:⁷
 - In October 2013, Woodring cut two power poles, used a tractor to pull down one of the poles, which severed a 115KV power transmission line resulting in loss of power to approximately 10,000 customers.
 - In September 2013, Woodring set fire to an electrical switching station resulting in substantial damages.

⁵ Lake Powell Life News, “Charges Brought Against Shooter of Garkane Energy Substation” (February 17, 2017), *available at* <https://www.lakepowelllife.com/charges-brought-against-shooter-of-garkane-energy-substation>.

⁶ Le Journal de Montreal, “Hydro wants a secret trial for the “star pilot” (January 9, 2017), *available at* <http://www.journaldemontreal.com/2017/01/09/hydro-veut-un-proces-secret-pour-le-pilote-des-stars>. *See also* Montreal Gazette, “Pilot’s attack on ‘spinal column’ of Hydro-Québec is unprecedented: lawyer” (October 31, 2018), *available at* <https://montrealgazette.com/news/local-news/pilots-attack-on-spinal-column-of-hydro-quebec-is-unprecedented-lawyer>.

⁷ FBI News, “Attack on Arkansas Power Grid” (August 10, 2015), *available at* <https://www.fbi.gov/news/stories/attacks-on-arkansas-power-grid/attacks-on-arkansas-power-grid>.

- August 2013, 500KV power lines fell on a nearby active rail line after being deliberately cut with over 100 support bolts removed from the 100 ft support tower where it was attached. The power lines were eventually struck by a train which led to a power outage affecting a substantial number of customers.
- In February 2014, three militia extremists in Georgia attempted to obtain pipe bombs and other explosives which they planned to use in guerilla warfare-style attacks. According to the criminal complaint, “‘the group’ was planning to ‘start the fight’ with the government by strategically planning to sabotage power grids, transfer stations, and water treatment facilities . . . this action would cause mass hysteria and if enough sabotage was successful, then martial law would be declared, therefore triggering other militias to join the fight.”⁸

12. On October 24, 2017, two individuals were arrested for breaking into a Kinder Morgan Trans Mountain Pipeline facility in the State of Washington in an attempt to shut the valve on the oil pipeline.⁹ One of the individuals involved posted a live feed of the attack on his Facebook page. The live feed was accompanied by a comment stating, “In honor of the one year anniversary of the Valve Turner’s actions, I ask that you join me in continuing their work.”¹⁰ Posted comments also

⁸ *United States v. Peace*, 4:14-cr-00011-HLM-WEJ (N.D. Ga. Crim. 2014) (see Criminal Complaint, dated February 18, 2014 at 6).

⁹ Goskagit.com, “Two arrested after apparent break-in at Kinder Morgan facility” (October 24, 2017), available at https://www.goskagit.com/news/local_news/two-arrested-after-apparent-break-in-at-kinder-morgan-facility/article_ab690b5c-1f7a-5402-a20b-4b1f56265cc2.html.

¹⁰ <https://www.facebook.com/donaldz/videos/10155315875063409/>. “Valve Turners” refers to a group of climate change activists.

included coordinates of valve stations in North Dakota, Michigan, Minnesota, and Florida urging others to commit similar attacks.¹¹

13. These recent posts highlight the need to keep the locations and configurations of critical infrastructure (electric or otherwise) offline because the Internet allows such information to be transmitted and shared instantaneously, anonymously, and to untold numbers of people.
14. Domestic and international intelligence communities have also reported on the use of the Internet for terrorist pre-operational planning. In 2012, the United Nations Office on Drugs and Crimes published a report entitled “The use of the Internet for terrorist purposes,” stating:

*Some sensitive information that may be used by terrorists for illicit purposes is also made available through Internet search engines, which may catalogue and retrieve inadequately protected information from millions of websites. Further, online access to detailed logistical information, such as real-time closed-circuit television footage, and applications such as Google Earth, which is intended for and primarily used by individuals for legitimate ends, may be misused by those intent on benefiting from the free access to high-resolution satellite imagery, maps and information on terrain and buildings for the reconnaissance of potential targets from a remote computer terminal.*¹²

15. Aside from government entities, activists have themselves admitted that publicly available data can be used for pre-operational planning of an attack on a pipeline. In 2014, activist Tom Steyer commissioned a three-month study, conducted by former Navy SEAL David M. Cooper, which concluded:

Keystone XL was an especially attractive target for terrorists . . . Cooper said he conducted the study by using publicly available information that anyone planning a terrorist attack could find, relying on such sources to determine Keystone XL's path and the thickness of

¹¹ *Id.*

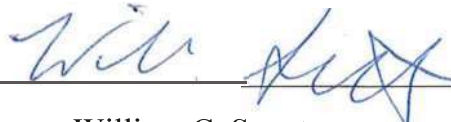
¹² United Nations Office on Drugs and Crime, “The use of the Internet for terrorist purposes” at 10-11, available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

*the pipe.*¹³

16. Given the potential consequences of an attack on the electric system, SDG&E considers electric system location and configuration data, such as information contained within the PV RAM maps and DRP access portal (as those acronyms are defined in the Joint Petition for Modification), to be safety- and security-sensitive information that should not be made publicly available.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed: December 7, 2018



William C. Sauntry

¹³ Portland Press Herald, “Study: Keystone XL pipeline would be juicy terrorist target” (June 5, 2014), available at <http://www.pressherald.com/2014/06/05/study-keystone-xl-pipeline-would-be-juicy-terrorist-target/>.