

**Enclosure 1 – SED Incident Investigation
Report, dated August 26, 2015**

CALIFORNIA PUBLIC UTILITIES COMMISSION
Safety and Enforcement Division
Incident Investigation Report

Report Date: 8/26/15

Incident Number: E20140827-01

Utility: Pacific Gas and Electric (PG&E)

Date and Time of Incident: 8/26/14, 2210 hours, to 8/27/14, 0241 hours

Location of Incident: 150 Metcalf Rd
San Jose, CA 95138
County: Santa Clara

Summary of Incident:

On August 26-27, 2014, PG&E's Metcalf Substation was burglarized by unknown suspects. The suspects breached the fence and stole construction equipment from the staging yard and the substation operations yard. PG&E reported that approximately \$40,000 in equipment was missing from the substation. SED's investigation found many gaps in PG&E's security management and lack of training for on-site personnel and security management.

Fatality/Injury: None reported

Property Damage: \$40,000 in stolen equipment

Utility Facilities involved: Metcalf Substation – construction equipment and perimeter fence

Witnesses:

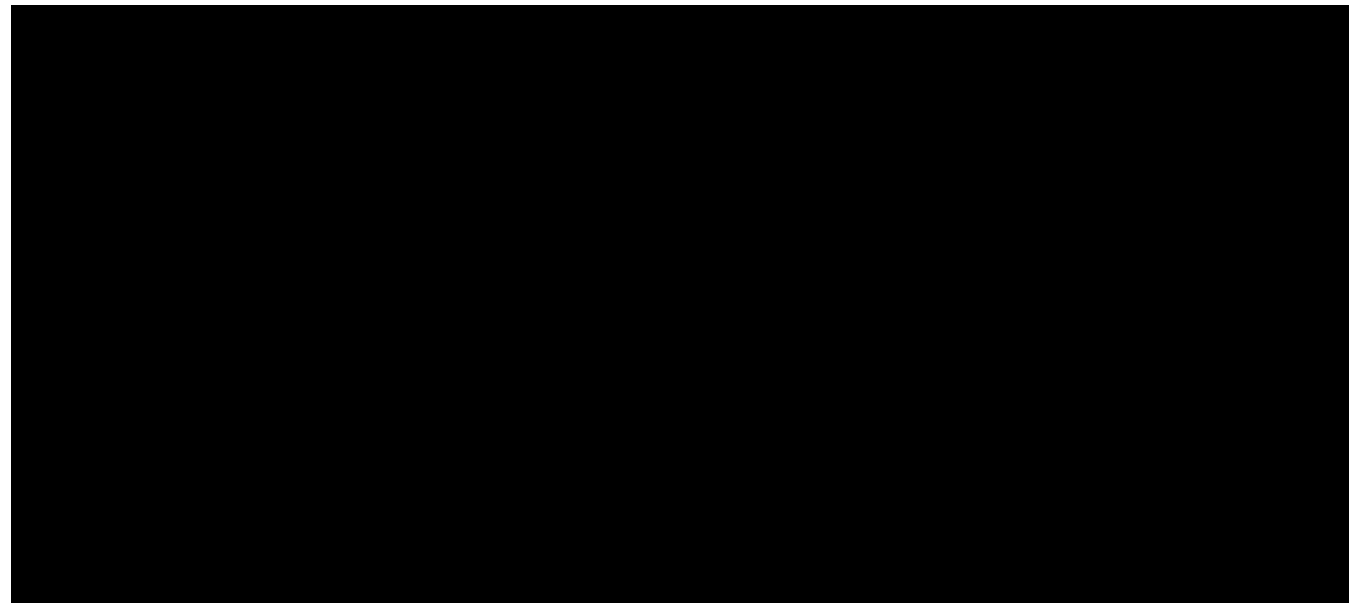
	<u>Name</u>	<u>Title</u>	<u>Phone</u>
1.	██████████	PG&E Supervisor, Regulatory	██████████
2.	██████████	PG&E Investigator 1, Corporate Security	
3.	Meredith Allen	PG&E Director, Regulatory	██████████
4.	██████████	PG&E Investigator 2, Corporate Security	██████████
5.	Evermary Hickey	PG&E Director, Emergency Preparedness	██████████
6.	Sergeant Bryan Glatz	Sheriff's Investigator, Santa Clara Sheriff	408.808.4400
7.	Raymond Cho	CPUC, SED Investigator	415.703.2236

Evidence:

	<u>Source</u>	<u>Description</u>
1.	PG&E	Initial Online Incident Report 8/27/14
2.	CPUC	Field Visit with Photographs 8/28/14
3.	CPUC	Data Request 1 on 8/28/14
4.	PG&E	Response 1 on 9/4/14
5.	PG&E/CPUC	Meeting debrief at CPUC 9/5/14
6.	CPUC	Letter to PG&E 10/3/14
7.	PG&E	Root Cause Analysis 11/21/14
8.	CPUC	Call with Sgt. Bryan Glatz 12/15/14
9.	CPUC	Data Request 2 on 3/20/15
10.	PG&E	Response 2 on 4/15/15
11.	PG&E	Supplemental Response 2 on 5/22/15

Observations and Findings:

Multiple alarms sounded at various times between 2210 hours on August 26, 2014, and 0241 hours on August 27, 2014, at PG&E's Metcalf substation. The alarms were the result of intruders who forced their way into the general construction (GC) yard next to Metcalf Substation, and two substation yards. The yards were burglarized of construction equipment valued at almost \$40,000. Although [REDACTED] sensors [REDACTED] alerted PG&E's employees and [REDACTED] of the intruders, their review of surveillance camera feeds did not show the intruders. It was not until 0600 hours on August 27, that PG&E's construction crews noticed [REDACTED] breaches in the fence as shown in figure 1. PG&E corporate security further inspected the site and found several containers were also accessed by force. PG&E did not report any impact on the electrical grid or any customer outages. The table in Appendix A chronologically summarizes key events for this incident.



On August 28, 2014, SED's investigator visited the Metcalf Substation, met with PG&E Investigator 2 [REDACTED] and Regulatory Supervisor [REDACTED] to debrief them regarding the stolen construction equipment and breached fence. SED's investigator observed that the Northeast perimeter fence of Metcalf substation runs parallel to state highway 101 and is easily accessible through the dirt path. The Northwest perimeter fence surrounding the general construction yard is almost perpendicular to the highway and is also accessible through the dirt field. [REDACTED] breach points along the Northeast and Northwest perimeter fences (see Figure 1 above) that surround the construction yard and operations yard (230 kV yard) were found. The suspects could have accessed PG&E's property from the highway (see Figure 2).



Figure 2. (left) Repaired Northwest fence (facing highway 101 from West to East)

Figure 3. (right) [REDACTED] with trailer obscuring view (along Northwest fence)

During the field visit, it was observed that PG&E had set up surveillance cameras at various points along the perimeter fence. The intruders cut the fence at strategic places behind a trailer and under a tree (see Figure 3). The other two locations were within sight of the security cameras. However, PG&E employees indicated that they were not aware of the intruders until after the incident had occurred. When the alarms sounded, PG&E security [REDACTED] and control center employees indicated that they reviewed the surveillance feeds and they could not confirm a security breach. [REDACTED]

[REDACTED] Evidence in the form of sheared pad locks and chain links led the investigator to believe a basic bolt cutter or metal shears were the tools used by the suspects to access the fence and the equipment containers. Containers as far as 800 feet away from the access point were forcibly opened. Metal thread shavings were observed outside the fence indicating the removal of a threading tool from the yard. PG&E is currently working with the Santa Clara Sheriff's Department as they conduct their own investigation to find the suspects.

SED's investigation revealed that at the time of the incident, [REDACTED] **failed to properly respond to alarms, and on-site personnel failed to routinely patrol the perimeter.** When [REDACTED] alarms were triggered, security staff did not adequately check different perspectives from the various cameras at either yard. PG&E employees [REDACTED] viewed the yards from at least three (3) different cameras and did not find any suspicious activity at that time. Thus, the security staff cleared the alarms once they found no evidence of entry. Camera feeds

were the only means used to verify the alarms instead of physically investigating the presence of any intruders. By clearing the alarm the intruders were allowed to continue surveying the substation for more containers to burglarize.

Security measures and equipment including perimeter [REDACTED] sensors, surveillance cameras, [REDACTED] lighting, and on-site patrol units were in place at the time of the incident. With security equipment in working order and a few cameras with an unobstructed view of the fence, the intruders took advantage of gaps (see summary of deficiencies below) in PG&E's security management and were able to cut the locks and access about six (6) different containers or trailers in both the GC and substation yards.

The following list summarizes all deficiencies discovered during the investigation:

- Lack of an accountable training procedure to verify security staff training (no records verifying training was completed)
- Lack of a proper preventative maintenance plan for security equipment (security equipment is not serviced)
- Insufficient security equipment and monitoring system [REDACTED]
- Absent supervising staff at critical substations (no supervisors to manage constant patrols)
- Absent security staff inside the substation (as opposed to perimeter management)
- Lack of PG&E Security Control Center staff [REDACTED]
- Breakdown in communication between on-site officers and control center staff [REDACTED]
[REDACTED]

The previous vandalism that occurred on April 16, 2013, at the same substation was enough to alert PG&E to possible gaps in its security policy, and that additional measures were necessary to physically protect its critical substations. However, PG&E failed to properly execute new countermeasures to protect its facilities, employees, and the electric grid. In this latest incident, the on-site guards should have been able to verify an actual intrusion by physically inspecting various facilities in the substation and contacting the local authorities for assistance. An intentional sounding of a certain security alarm could have stopped the intruders from continuing to explore the yard for more than four hours. If PG&E had properly calibrated the [REDACTED] sensors [REDACTED] to limit the number of [REDACTED] the company would have had a higher chance at thwarting this burglary or preventing it from happening.

After this incident, PG&E reviewed and improved its security management by taking the following measures: increased security personnel and re-established supervisor position at Metcalf Substation, mandated that routine patrols be closely monitored by supervisors, addressed gaps in security response protocol, enhanced security equipment (lighting and cameras), replaced [REDACTED], emphasized and re-evaluated training requirements, and conducted penetration testing (proactively

evaluating PG&E's security management for weaknesses). Additionally, PG&E received a permit to build an opaque wall on September 22, 2014 and has proceeded to construct the new wall around the perimeter of Metcalf substation.

In response to this incident, the SED requested that PG&E conduct a Root Cause Analysis (RCA) on the events leading up to the burglary. PG&E did so. The RCA report included: events that occurred during and following the August 26-27 incident, PG&E's hiring practices and management of third party contractors, protocols in place and how such procedures functioned during and following the incident, and all PG&E planned security countermeasures with implementation dates. PG&E submitted the confidential RCA to SED on November 21, 2014, along with a public Summary Report, which has been posted on the Commission's website. Contained in the Summary Report is a briefing of what transpired on April 16th and August 26th, along with measures to address gaps in security management and physical security enhancements. SED recommends that PG&E continue to adhere to PG&E's "Action Plan Summary" and complete improvements by the dates scheduled.

PG&E also presented to SED its security management action plan, outlined in the RCA report, which addresses the gaps in security mentioned above. PG&E plans to develop and implement a more robust training program for security staff to ensure a proper response to alarms, implement the use of human performance tools within the security control center, and develop a set of security policies and procedures for:

- Security guards
- Work performed at the control center
- Training requirements and tracking for security staff
- Maintenance and repairs for security systems

Recommendations:

SED recommends and expects PG&E to fully implement its security management action plan, as PG&E indicated. In implementing its plan, PG&E shall address the following:

- PG&E shall require that the security contractor patrol the perimeter routinely and perform a thorough inspection of the fence line at all times. Regardless of notifications from alarms, the patrol should have noticed activity within or outside of PG&E property. Although static camera feed positions were reviewed, cameras could have been [REDACTED] [REDACTED] for a more thorough investigation after the alarm sounded. **PG&E should place additional cameras that survey the blind spots of other cameras that could have aided in verifying the alarm.**

- PG&E's report of events also noted limited visibility [REDACTED] PG&E shall install [REDACTED] for each camera, or shall install cameras [REDACTED] to increase chances for validation of the alarm. [REDACTED]
- Personnel at the substation and within the PG&E security control center [REDACTED] [REDACTED] [REDACTED] [REDACTED] PG&E shall adequately train security management and on-site personnel to properly identify and respond to alarms.
- The alarm at Metcalf substation could be set off due to many reasons, [REDACTED] [REDACTED] Between 2200 hours on August 26 and 0300 hours on August 27, PG&E's security control center reported [REDACTED] [REDACTED] of these alarms occurred at Metcalf substation. [REDACTED] [REDACTED] [REDACTED] PG&E shall properly maintain security equipment [REDACTED] [REDACTED] sensors [REDACTED] should be calibrated and tested routinely.

Preliminary Statement of Pertinent General Order, Public Utilities Code Requirements and/or Federal Requirements:

PG&E failed to furnish and maintain its equipment and facilities at the Metcalf substation as required by Public Utilities Code section 451.

Conclusion:

The breach of security at PG&E substation was caused by several gaps in security management, including the lack of training, failing to identify blind spots [REDACTED] perimeter, inaction by security personnel [REDACTED] inadequate maintenance of security equipment, and a lack of suitable camera equipment and lights. PG&E has proposed measures to remedy all the identified gaps and to improve the security of substations. SED expects PG&E to fully implement the proposed measures and SED will continue to monitor PG&E's planned progress to ensure that all measures to harden physical security are completed in a timely manner.

Appendix A. Summary of Events at Metcalf Substation

Time (year/month/day:(hour))	Activity
2014/08/26:(2210-2252 hours)	[REDACTED] sensor triggers alarm three (3) separate times in General Construction (GC) yard adjacent to Metcalf Substation.
2014/08/26:(2302 hours)	Alarm is logged as false alarm by security [REDACTED] and PG&E security staff.
2014/08/26:(2349 hours)	A fourth alarm is experienced from the GC yard and is logged as a [REDACTED]
Next Day 2014/08/27:(0000 hours)	
2014/08/27:(0202 hours)	[REDACTED] sensor triggers first alarm (1) in Metcalf Substation yard.
2014/08/27:(0204 hours)	Security staff reviews live camera feed in the vicinity of alarm. Alarm cleared after staff found no activity.
2014/08/27:(0209-0218 hours)	[REDACTED] and are cleared as [REDACTED].
2014/08/27:(0218 hours)	[REDACTED] triggers second alarm (2) in Metcalf Substation yard and staff reviews recorded footage for 30 minutes.
2014/08/27:(02[REDACTED] hours)	Third alarm (3) experienced in Metcalf Substation yard.
2014/08/27:(02[REDACTED] hours)	Fourth alarm (4) experienced in Metcalf Substation yard.
2014/08/27:(02[REDACTED] hours)	Alarm cleared after no activity was verified after reviewing recorded footage.
2014/08/27:(02[REDACTED] hours)	Fifth alarm (5) experienced in Metcalf Substation yard.
2014/08/27:(02[REDACTED] hours)	Sixth alarm (6) experienced in Metcalf Substation yard.
2014/08/27:(02[REDACTED] hours)	Seventh alarm (7) experienced in Metcalf Substation yard.

2014/08/27:(02[REDACTED] hours)	Eighth alarm (8) experienced in Metcalf Substation yard.
2014/08/27:(02[REDACTED] hours)	Camera #7 (in vicinity of alarm) is reviewed and operator does not observe activity.
2014/08/27:(02[REDACTED] hours)	Ninth alarm (9) experienced in Metcalf Substation yard.
2014/08/27:(02[REDACTED] hours)	Tenth alarm (10) experienced in Metcalf Substation yard.
2014/08/27:(02[REDACTED]-02[REDACTED] hours)	Alarm is triggered in GC Yard. Staff reviews the camera feeds and finds [REDACTED] tripped the [REDACTED] alarm. Alarm is cleared.
2014/08/27:(0600 hours)	A substation construction foreman notices a cut in the fence and notifies his supervisor.
2014/08/27:(0713 hours)	The construction supervisor reports the breach to PG&E Corporate Security and calls Santa Clara County Sherriff's Office.
2014/08/27:(approximately 0730 hours)	Santa Clara County Sherriff's investigator arrives at Metcalf Substation.
2014/08/28: (0945 hours)	SED staff (Raymond Cho) arrives at Metcalf Substation to investigate.