

Summary Report for Electric Incident Review

Metcalf Substation

As requested by the Safety and Enforcement Division of the California Public Utilities Commission (CPUC), Pacific Gas and Electric Company (PG&E) is providing a root cause analysis about the burglary that occurred at the Metcalf substation in August 2014, including an overview of the actions and enhancements the company has put in place since the initial April 16, 2013, attack on the facility.

Substation physical security is one of the most important issues facing grid operators and PG&E understands how imperative it is to implement strong measures to protect critical substations. PG&E is currently in the first year of a three-year plan to invest more than \$100 million to significantly upgrade security at our critical facilities following last year's attack. Major elements of the plan related to physical security were in the process of being implemented at the time of the August burglary. However, some security measures that are part of our plan are still in process and were not in place to help prevent it.

The burglary that occurred at the Metcalf facility in August 2014 underscored the need for additional focus on training and supervision to support the work being done to upgrade technology and physical deterrents at facilities. As a result, PG&E is reprioritizing training and augmenting security supervision to prevent a similar incident.

The root cause analysis contains detailed, confidential information about aspects of the security measures PG&E takes at its facilities and has therefore been sent to the CPUC under confidential protection. Given the appropriate need for the public to have access to information about the two incidents and the steps PG&E is taking to safeguard critical infrastructure, PG&E has developed this public summary report to outline the company's findings.

This summary report includes:

- An overview of the events around the April 16, 2013, Metcalf attack;
- Action steps taken after the April 16, 2013, Metcalf attack;
- An overview of the events around the August 26 - 27, 2014, Metcalf burglary;
- Synopsis of the root cause analysis performed by the company after the August 26 – 27, 2014, Metcalf burglary; and
- Additional action steps taken since the August 26 – 27, 2014, Metcalf burglary.

April 2013 incident at Metcalf Substation and Countermeasures Taken

April 16, 2013, Incident Overview:

On April 16, 2013, gunshots caused extensive damage to the Metcalf Transmission Substation south of San Jose. No one was hurt and no customers lost power as a result of this incident. PG&E's Transmission Control Center operators reacted to alarms and worked to avoid service interruptions for PG&E's customers. Crews also arrived on site to assess the full impact of the damage and begin repairs. PG&E's electric system contains significant redundancies that allow the company to reroute and shift electric load when equipment is damaged. Those redundancies worked as designed.

Following the incident, PG&E worked with federal, state and local agencies, as well as outside consultants to take interim steps to improve substation security while developing a three-year plan to enhance security at critical substations:

- PG&E deployed security guards to provide 24/7 presence at critical substations and increased patrols from local law enforcement;
- PG&E trimmed back vegetation undergrowth around substations to remove potential hiding places; and
- At Metcalf specifically, PG&E installed temporary measures to shield equipment, enhance lighting and obstruct views into the facility while more permanent measures are being designed and engineered.

Additional physical security measures PG&E is currently taking include, among others:

- Opaque or solid walls around the perimeter to shield and obstruct views of equipment inside the substation;
- Enhanced detection and deterrent systems; and
- Improved lighting and camera systems.

PG&E has also worked with law enforcement and industry stakeholders to share information and take appropriate actions on an ongoing basis to protect its facilities.

April 16, 2013, Summary of Actions Taken:

Following the April 2013 attack at the Metcalf substation, PG&E began an assessment and developed a three-year plan to invest more than \$100 million to enhance security at its highest priority facilities. Some of the actions taken by PG&E included:

- Worked with local law enforcement to increase security presence at Metcalf and additional facilities (completed within 24 hours of the incident);
- Contracted with a private security company to provide 24/7 security officer coverage (completed within 24 hours of the incident);
- Installed portable lighting (completed within 30 days of the incident);
- Installed temporary fencing (completed within 30 days of the incident);
- Contracted with security consultants to conduct security assessments (completed within 30 days of the incident);
- Completed a series of tours of critical substations with law enforcement agencies. Latitude and longitude coordinates were issued to law enforcement aviation units for aerial patrol when available (June 2013);
- Developed and distributed briefing “tailboards” to employees at major substations to discuss security procedures and suspicious activity reporting (July 2013);
- Received approved permits and removed vegetation surrounding Metcalf (August 2013);
- Initiated an internal training program which included suspicious activity reporting and awareness (September 2013);
- Made improvements to the “Suspicious Activity Reporting” system in Corporate Security (October 2013);
- Participated in an industry and law enforcement sharing campaign in conjunction with the Department of Homeland Security, the Federal Energy Regulatory Commission, North American Electric Reliability Corporation and the Federal Bureau of Investigation. Events were held in each of the 10 Federal Emergency Management Agency jurisdictions (November 2013);
- Initiated an effort to formalize existing policies and procedures associated with the PG&E security system (March 2014);
- Conducted an assessment and test of current security systems at Metcalf (March 2014);
- Enhanced camera surveillance at Metcalf (April 2014);

- Announced a \$250,000 reward for information leading to the arrest and conviction of the individual(s) responsible for the attack on the anniversary of the incident (April 2014);
- Worked with local law enforcement to provide enhanced security awareness on the anniversary of the Metcalf event (April 2014);
- Contracted with security consultant to evaluate and provide recommendations for processes and procedures at PG&E's security control center (June 2014);
- Invited Department of Homeland Security to perform a security assessment at Metcalf in coordination with PG&E (June 2014);
- Released a Job Bulletin for additional operators at PG&E's security control center (July 2014);
- Performed on site post order training with security personnel at Metcalf (August 2014);
- Enhanced perimeter lighting at critical locations with additional portable lighting at Metcalf (September 2014);
- Received permit and began construction on a solid wall around Metcalf (September 2014);
- Published Utility Procedure for Security Control Center Alarm Response (September 2014);
- Published Utility Procedure for Security Control Center Incident Response (September 2014); and
- Briefed alarm and incident response protocols and trained security operators on revised response protocols (September 2014).

There were a number of other initiatives that were in the process of being implemented as part of PG&E's security plans when the August 26 – 27, 2014, Metcalf burglary occurred.

August 2014 Burglary at Metcalf Substation, Root Cause and Summary of Actions Taken

Incident Overview

Prior to the August 2014 Metcalf burglary, PG&E's actions to mitigate security threats were mainly focused on upgrading the physical security measures of the company's substations as part of an overall plan to enhance security at substations.

Between the hours of 22:10 on August 26, 2014, and 02:41 on August 27, 2014, PG&E's Metcalf facility was the site of unauthorized entry. As a result of the intrusion, approximately \$38,651 of construction tools and equipment was taken.

Despite detection by both the third-party video monitoring system and other security measures, the thefts were not identified until 06:00 hours on August 27, 2014, when construction crews arrived for work.

August 26 – 27, 2014, Summary of Actions Taken

Immediately following the August 2014 burglary, PG&E took numerous initial actions to address security gaps at the facility, including:

- Secured Metcalf Substation fence damaged during the burglary (completed within 24 hours of the incident);
- Checked all equipment within substation for operational damage and found none (completed within 24 hours of the incident);
- Increased security officer presence on site (completed within 24 hours of the incident);
- Enhanced portable lighting onsite (completed within 48 hours of the incident);
- Reinforced and checked to ensure that roving patrols were occurring within Metcalf Substation (completed within 30 days of the incident);
- Re-established onsite roving supervisor position (completed within 30 days of the incident);
- Addressed alarm and incident response protocols for security operations center personnel (completed within 30 days of the incident);
- Performed security review and penetration testing at Metcalf substation (October 2014);
- Enhanced camera systems at Metcalf (October 2014);
- Replaced 3rd party guard contractors (November 2014); and
- Replaced security operations contractors and increased staffing and supervision (November 2014).

Root cause analysis findings

PG&E also assembled an experienced and multi-disciplinary team from across the company to conduct a root cause analysis of the August 2014 incident. The team's root cause analysis, which is submitted in a separate confidential document, found that the security breach was due to the following direct and root causes:

- **Direct Cause:** PG&E's security control center failed to properly respond to alarms and the on-site security officers failed to follow clearly delineated post orders requiring them to perform continuous patrol of Metcalf Substation.
- **Root Cause:** Inadequate training and supervision, created an environment in which PG&E's Security Control Center personnel and on-site security officers failed to follow delineated procedures and post orders.

Additional Actions Planned Based on Root Cause Analysis (Subset of Actions Planned)

As a result of findings outlined in the root cause analysis, PG&E is taking additional actions in a timely manner to prevent a similar incident from occurring. Additional actions include, among other measures:

- Developing and implementing a robust training program for security officers to ensure that alarms are responded to effectively;
- Implementing the use of human performance tools within security control center operations;
- Developing a comprehensive set of security policies and procedures for:
 - Security guards;
 - Work performed at security control center;
 - Training requirements and tracking process for security operators and officers; and
 - Maintenance and repairs for security systems.

Conclusion

PG&E and the utility industry have taken significant steps to increase security following the Metcalf substation attack in April 2013. Although much work had been done to increase physical security at facilities following the incident, the subsequent burglary in August 2014 shows that training and supervision were inadequate to ensure procedures were consistently followed.

PG&E is committed to addressing training and supervision along with other issues raised by the root cause analysis, while continuing to work closely with regulators and law enforcement to maintain the security of the company's facilities.