Enclosure 3 – PG&E Root Cause Analysis (RCA)

2014 Internal Electric Incident Review

Metcalf Substation Unauthorized Entry 8/27/2014

Executive Summary:

Between the hours of 2210 on 8/26/2014 and 0241 on 8/27/2014, PG&E's Metcalf facility was the site of two unauthorized entries. The first occurred in the General Construction (GC) yard adjacent to the Substation, and the second occurred in the Metcalf Substation. As a result of the intrusions, $38,651 of construction tools was lost. At the time of the intrusions, Metcalf was equipped with the following security measures:

- fencing [redacted]
- perimeter [redacted] detection
- [redacted] video and alarm monitoring [redacted]
- [redacted] lighting
- [redacted] access control
- [redacted] on-site private security officers with post orders to perform continuous patrols of the site perimeter

Despite detection by both the [redacted] video monitoring system and the PG&E security measures, the thefts were not identified until 0600 hours on 8/27/2014 when the construction crews arrived for work. The thieves were allowed to continue undeterred due to several issues, including:

- A lack of effective training for PG&E's Security Operators
- On-site security officers not following post orders
- Inadequate processes and procedures for alarm response for both the [redacted] video monitoring system and PG&E's Security Control Center

In addition, there were a number of other issues identified that contributed to the event. Both the alarm and training issues were identified in previous evaluations following the security incident that occurred on 4/16/2013 at Metcalf Substation, and remedial measures had been targeted to be completed by Q4 2014.

Table of Contents:

Metcalf Substation Security Breach

General Information:

Title of Incident	Metcalf Substation Security Breach
Incident Date	8/27/2014
Incident Time	0202 hours
Number of Customer Affected	N/A
Customer Outage Minutes	N/A
Duration of Restoration	N/A

Investigative Approach: Root Cause Analysis of Alarm System Performance, Human Performance, Supervisory, individual and organizational factors are analyzed to identify those corrective actions to prevent recurrence.

Review Team:

Name	Position/Title
[redacted]	Supervisor, EO-TO-TBO-Work Methods & Procedures Group
[redacted]	CAP Supervisor, PG Hydro O&M
[redacted]	Manager, Performance Improvement
[redacted]	Security Investigator, Corporate Security
[redacted]	WPE Specialist EO-TO-TBO-Work Methods & Procedures Group

Individual Contributors:

Name	Position/Title
[redacted]	Sr. Advisor, Security Project, Corporate Security
[redacted]	Security Investigator, Corporate Security
[redacted]	Security Control Supervisor, Corporate Security
[redacted]	Physical Security Spec., Sr., Corporate Security
[redacted]	Manager, Security Operations, Corporate Security
[redacted]	Security Investigator, Corporate Security
[redacted]	Sr. Security Investigator, Corporate Security
[redacted]	Contract Management Supervisor, EO-TO-TOS Contract Mgmt
[redacted]	Manager, Asset and Executive Protection

[redacted]	Contract-Sr. Project Manager
Stephanie Douglas	Director, Corporate Security
[redacted]	Physical Security Specialist
[redacted]	[redacted] Security Control Operator

Abbreviations/Acronyms:

CIP	Critical Infrastructure Protection
CSD	Corporate Security Department
DHS	Department of Homeland Security
GC	General Construction
GCC	Grid Control Center
GRC	General Rate Case
LOB	Line of Business
NERC	North American Electric Reliability Corporation
PSIM	Physical Security Information Management
PTZ	Pan Tilt Zoom
RFP	Request for Proposal
SAR	Suspicious Activity Report
SCCSO	Santa Clara County Sheriff's Office
SVA	Site Vulnerability Assessment
TBO	Transmission Business Operations
TO	Transmission Operations
WM&P	Work Methods and Procedures
WPE	Work Procedure Error

Investigation Objectives:

The objectives of this investigation are to:

- Identify the root and contributing causes of the failure to validate alarms at Metcalf Substation.
- Formulate an action plan to prevent the recurrence of similar events.

NOTE: Throughout this review, individuals will be referred to by classification, not by name.

Description of the Event:

Security systems in place at Metcalf Substation at the time of the event included:

- fencing [redacted]
- perimeter [redacted] detection
- [redacted] video and alarm monitoring
- [redacted] lighting
- [redacted] access control
- [redacted] on-site private security officers with post orders to perform continuous patrols of the site perimeter

Beginning at 2210 hours on 8/26/2014, multiple alarms were generated in the General Construction (GC) yard adjacent to Metcalf Substation. This yard is not within the security perimeter of Metcalf Substation [redacted] The GC Yard is currently being monitored [redacted]

[redacted], PG&E's Security Control Center received [redacted] an alarm in the GC yard. Metcalf Substation is patrolled by contract security officers. PG&E's Security Control Center contacted the on-site security officers assigned to Metcalf Substation who confirmed that [redacted] on-site security [redacted] were present at Metcalf. No action was taken by the on-site security officers in response to the call from PG&E's Security Control Center.[1] No additional action was taken by the operator [redacted] video monitoring system [redacted]

At 2349 hours, the [redacted] video monitoring system received an additional alarm in the GC yard, but the operator of the [redacted] video monitoring system did not [redacted] and logged the alarm as "Alarm caused by material shifting," with the alarm resolution logged as "False Alarm."

At 0202 hours on 8/27/2014, security was breached at Metcalf Substation. PG&E's Security Control Center received a perimeter Metcalf Sub, Fence Zone [redacted] alarm. The perimeter alarm and camera system

[1] Interviews with the security officers both at PG&E's Security Control Center and on-site at Metcalf identified discrepancies in the conversation regarding if any actions were requested from the on-site security officer. The discrepancy cannot be resolved because there is no [redacted]

operated as designed for the intrusion, with cameras [redacted] to the detection site and multiple alarms sent to PG&E's Security Control Center.

In response, the security operator on duty at PG&E's Security Control Center attempted to validate the alarms. [redacted] No activity was observed,[2] and the operator cleared the alarm from the alarm page.

At 0209–0218 hours, the operator at PG&E's Security Control Center monitored other incoming [redacted] alarms [redacted] PG&E's Security Control Center receives [redacted] alarms. On the night of this event, between 2200 and 0300 hours, [redacted] alarms received, from various locations. When the operator received the first Metcalf alarm at 0202 hours, s/he focused on it [redacted]

At 0218 hours, a second Metcalf Sub, Fence Zone [redacted] alarm was received at PG&E's Security Control Center, and the operator [redacted] Metcalf Substation camera [redacted] mode. The operator reviewed the [redacted] image [redacted] with no activity observed.[3] The operator cleared the alarm from the alarm page.

At 0241 hours, after receiving [redacted] additional alarms from Metcalf Sub, Fence Zone [redacted] the operator [redacted] camera [redacted] and viewed the [redacted] the camera. No activity was observed, and the operator cleared the alarm from the alarm page.

In total, there were [redacted] Metcalf Sub, [redacted] Zone [redacted] alarms over the course of 41 minutes.

At 0600 hours, a Substation Construction foreman saw the cut in the fence and notified his supervisor.

At 0713 hours, PG&E's Corporate Security Department (CSD) was notified of the event (1 hour 13 minutes after the break-in was discovered).

At 1052 hours, the Grid Control Center (GCC) was notified of the event (4 hours 52 minutes after the break-in was discovered).

As a result of the intrusions, $38,651 of construction tools was lost.

[redacted]

Alarm System Findings:

All security equipment at Metcalf Substation worked as designed.[4] However, our review of the event revealed the following issues:

- Existing video cameras require [redacted]
- The perimeter alarm system is [redacted]
- The current alarm systems have corrective maintenance plans but [redacted] place to ensure they function as designed.

Policies and Procedure Findings:

Our review of the event revealed two issues regarding compliance with policies and procedures:

- PG&E's "Response to Access Control Alarms" (dated 6/21/12) requires PG&E's Security Control Center [redacted] Although PG&E's Security Control Center [redacted] they failed to [redacted]

- PG&E's Procedure TD-3463P-01 (Substation Entry, Threats, Inspection and Maintenance for Physical Security) requires that all employees entering substations perform visual surveys of the facilities for any signs of vandalism or abnormal conditions and report abnormal findings to the control center(s) having jurisdiction. The substation construction foreman who discovered the break-in performed the visual survey but did not contact the Grid Control Center (GCC).The GCC was contacted by a substation electrician who arrived on scene 4 hours and 52 minutes after the break-in was discovered.

Training Findings:

Pursuant to PG&E's contract with the security vendor, the following training is required:

- 4.2.1 The Facility Manager, along with the support of the Supervising Lieutenant, has the responsibility of ensuring that training of new hires and existing employees on staff is completed and provided to Corporate Security. It is important that the trainee be trained on the duties of the position they are assigned.
- 4.2.2 New officers will be [redacted] trained as follows, as applicable to the facility location:
  - Walk-through facility briefing on and observing all applicable areas,

[4] The perimeter alarm system at Metcalf Substation, having sustained damage in the 2013 security incident, was repaired and calibrated in July 2013.

- Read the Post Orders,
- Train in detail all procedures, then the new Security Officer will demonstrate to the instructor knowledge and comprehension of the procedures,
- Retrain all areas not fully understood by the new Security Officer,
- Complete a post-training checklist,
- Complete [redacted] of training on facility system before manning a post [redacted]

Our review of the event revealed the following issues with training:

- Existing training for security operators at PG&E's Security Control Center consists of a two-week period where new employees are observed by a seasoned operator. At the time of this event, there were no documents at PG&E's Security Control Center indicating that security operators had received any training for their duties while on shift or that individual security operators had demonstrated proficiency in the use of the tools available to them to fulfill their duties.
- Under the terms of PG&E's [redacted] training of PG&E's Security Control Center operators was to be performed by the security [redacted] However, there was no documented process in place to verify operator training.

Environment Findings:

Our review of the event revealed the following environmental issues:

PG&E's Security Control Center employees have many responsibilities, including but not limited to:

- Responding to and evaluating all security alarms
  - video surveillance
  - video alarms
  - [redacted] alarms
  - access alerts

[redacted]

PG&E's Security Control Center started with [redacted] cameras and has expanded to [redacted] and grows monthly. It has incrementally expanded its staff, scope and volume of services over subsequent years on an as-needed basis. PG&E's Security Control Center has numerous physical and operational challenges, including but not limited to:

- Small working space

[redacted]

- Numerous technological demands such as:

- [redacted] video surveillance from digital video recorders in various sites [redacted]

People Findings:

Our review of the event revealed the following findings related to people:

- The on-site security officer at Metcalf had clearly defined post orders that required continuous patrols of the site perimeter. The security officers on duty that night did not perform the patrols of the site perimeter.
- Review of the video shows the cameras reacted appropriately to the [redacted] alarms; however, no operator response/control was observed. [redacted]
- There were [redacted] security operators at PG&E's Security Control Center on duty the night of the incident. At the time of the incident, one operator was on lunch break and was not a part of the response. The operator that was monitoring the Metcalf Zone [redacted] alarms [redacted]
- At the time of the event, there was no supervisor on shift at the Security Control Center when the incident occurred.
- A number of [redacted] lighting units installed at Metcalf substation after the April 2013 incident had been removed due to complaints from neighbors, which reduced illumination of the surrounding area. While the break-in did not occur where the lighting was removed, [redacted] This decision was made by the LOB without consultation of [redacted]

Management Systems Findings:

Metcalf Substation was the site of a previous security incident that occurred on 4/16/2013. Following the incident, PG&E conducted an assessment of the security at Metcalf Substation, as well as an evaluation of PG&E's Security Control Center's systems, which provided recommendations for improvement.[5]

One of these recommendations was to develop a comprehensive set of security policies and procedures. Since the earlier Metcalf incident, the major short-term focus has been on physical security upgrades to Metcalf Substation. Development of policies and procedures was slated to be completed by Q4 2014.[6]

CSD has experienced an expansion of its roles and responsibilities in addition to its traditional role over physical security. The increase has been largely driven by North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements, such as increased video monitoring, site access, investigations and management of security system issues.

With respect to PG&E's hiring and management of security [redacted] PG&E utilizes a [redacted] and for field security personnel. The established [redacted] mandates the contract company's responsibilities to maintain Standards of Conduct, Training Requirements, Post Orders, and Guard Responsibilities for [redacted] and stationary field locations. The contract language requires the contractor to provide supervision by professional attentive management who shall be available to the PG&E representative at all times during the performance of work. Management of PG&E's Security Control Center [redacted] falls within the responsibility of the Corporate Security Department, with support from the [redacted] while funding of the on-site security contractors at the substations falls within the responsibility of Electric Operations.

[5] Following the April 2013 incident at Metcalf, PG&E has completed a number of corrective actions designed to enhance security of the facility. A summary of these actions is in Attachment – 14.

[6] In March 2014, an Operational Risk Analyst was hired by the Corporate Security Department (CSD) to work on documentation of processes and procedures for the department. Formal work on documentation of policies and procedures for PG&E's Security Control Center began in April 2014, and procedures for specific alarm response in regard to [redacted] sites and third party communications were published on 9/16/2014. In addition, CSD hired a third-party consultant to write formal process, procedure, training and job aids for PG&E's Security Control Center in July 2014. Work on this task is ongoing.

Event Causes:

Direct Cause –

PG&E's Security Control Center failed to properly respond to Metcalf Zone [redacted] 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.

Contributing Causes –

Alarm Systems:

- The perimeter alarm system is [redacted]
- Technologies in use at the Security Control Center consist of [redacted] during alarm response [redacted]
- Camera systems do not provide [redacted]
- The lack of preventative maintenance to service and clean camera systems contribute to degraded images [redacted]

Policies and Procedures:

- At the time of the event, PG&E did not provide clear direction to employees [redacted] at the Security Control Center regarding [redacted] site alarm response and [redacted] communication.
- Although the contract security company completed a document titled "Security General Orders" for the PG&E Security Control Center in May 2013, there is no evidence that this document was utilized.

Training:

- PG&E's Security Control Center operators' training was to be performed by [redacted] but there was no documented process in place to verify that the operators were trained to key skills to fulfill their duties, including [redacted] and utilizing [redacted]
- Metcalf security officers, immediately following the April 2013 event, conducted patrols within [redacted] of the substation. The contract security officers were later restricted [redacted] due to a lack of training [redacted] This limited the ability of the on-site security officers [redacted]

- Neither the control center security operators nor the onsite security officers were trained in the use of 3-way communications. The use of 3-way communications would have decreased the likelihood of the type of miscommunications that contributed to this event.

Environment:
PG&E's Security Control Center employees have numerous responsibilities as well as numerous physical and operational challenges such as but not limited to:

- There are [redacted] computer software systems in use. In some instances, upon receipt of an alarm, operators must either [redacted] Physical Security Information Management (PSIM), a commercially available software platform designed to integrate multiple unconnected security applications, would allow control of all systems through one user interface and ease some of the workload for the security operators by identifying, prioritizing, and tracking alarms.
- The security operators have a very high workload. [redacted] A major contribution to this workload is [redacted] that typically come from perimeter [redacted] and are a direct result of a lack of maintenance to the systems.
- This event occurred during the hours of darkness [redacted] Technology is available to [redacted] mitigate this issue.

People:
- The post orders for the on-site officers required constant patrol of the perimeter of the substation to detect fence and building intrusion. This did not occur on the night of the event and may be attributed to a lack of supervision.
- The security operator at PG&E's Security Control Center did not complete the tasks necessary to fulfill his/her duties, such as [redacted] and contacting the on-site security [redacted] to investigate the cause, suggesting a lack of training.
- The security operator that was monitoring the Metcalf alarms had not been briefed [redacted] indicating a lapse in communication.

Management:

- Following the security incident that took place on 4/16/2013, PG&E conducted an assessment of the security at Metcalf Substation, as well as an evaluation of PG&E's Security Control Center's systems. The major short-term focus has been on physical security upgrades to Metcalf Substation. Development of policies and procedures was slated to be completed by Q4 2014.
- The Security Control Center is a 24-hour/7-day-a-week facility staffed by [redacted] employees. The PG&E [redacted] provides for supervisor oversight although there is [redacted] When the incident occurred, a single PG&E employee served as a functional supervisor and liaison to the [redacted] without clearly defined roles and responsibilities. The majority of time spent by the PG&E employee was related to processing of access requests. The investigation identified a situation where direct supervision of the [redacted] employees did not exist for all shifts.
- As noted above ("Environment"), the current alarm systems do not have preventative maintenance plans to ensure they function as designed. [redacted] Currently, each Line of Business (LOB) is responsible for maintenance of security systems. Because the LOB's have competing priorities for available expense funding, long delays to maintenance and repairs of security systems have occurred.
- The roles and responsibilities for CSD as a whole have increased significantly over time, including taking over responsibility for physical security at PG&E's facilities. Most recently, the increase has been largely driven by NERC CIP requirements, such as increase of video monitoring, site access control, investigations and management of security system issues. Many of the contributing causes described above, such as inadequate oversight of security officer contracts, maintenance of security systems, technology upgrades, and resources to develop policies and procedures, may be attributable to the fact that responsibility for management and funding of these activities has historically fallen under the LOBs rather than under CSD .
- On 2/14/2014, the Roving Security Officer Supervisor position was removed, limiting checks on security officers to random spot checks by CSD. This decision appears to have been influenced by pressures associated with a need for supervision versus unbudgeted expenses. The absence of a Roving Security Officer Supervisor may have contributed to the failure of the onsite security officers to follow their post orders on the night of the incident. Immediately following the August 2014 incident, the roving supervisor position was re-established. As of 11/15/14, [redacted] roving supervisor positions have been created and filled.

Supplementary Observations:

During the course of this investigation, the following information was discovered which merits further review and possible action.

- The existing logging system at the Security Control Center is not [redacted]
- Phone lines at the Security Control Center are [redacted] which prevents validation of verbal conversations and any directions that are given. [redacted] phone lines provides a means of monitoring for procedural adherence, time stamped evidence for incident investigation and data for training purposes.
- The "Procedure for Alarm Response to [redacted] Sites" is not linked to Utility Procedure: RISK-1001P-05 - Security Control Center Alarm Response Procedure.
- In 2010, a need was identified to [redacted] at the Security Control Center, including installation of a Physical Security Information Management system (PSIM).Based on the results of outside reviews of the Security Control Center conducted following the April 2013 incident, PG&E prioritized action on the PSIM project. CSD successfully conducted a request for proposal in February 2014, interviewed vendors and had scheduled a proof of concept with vendors in September 2014. CSD has since chosen a product, identified funding and initiated a project plan. Steps should be taken to track and ensure completion.
- To provide redundancy to PG&E's Security Control Center, an alternate Security Control Center was created in [redacted] At the time of this investigation, we were unable to confirm if all electrical systems required for operation of the alternate Security Control Center are [redacted] or to locate a documented activation plan for the alternate site.

During review of the PG&E Security Control Center, the utilization of Human Performance Error Preventions Tools was absent. Human Performance Tools such as "3-Way Communication" would ensure correct directions are acknowledged.

Conclusion:

Although this event is a result of individual human failures, those failures can be attributed to a lack of CSD management focus on supervision, training and the development of policies and procedures. This is demonstrated by:

1. Security Operator Training was not verified by PG&E. Although several documents were identified that referenced training required for security operators, at the time of this event there were no documents at the Security Control Center indicating the security operators had received any training. There were no documents at Security Control Center indicating individual security operators had demonstrated proficiency in the use of the tools available to them to fulfill their duties.

2. PG&E did not ensure adequate supervision occurred as delineated in the [redacted] for the security operators. Additionally, the Roving Security Officer Supervisor position was removed, limiting the verification of compliance with post orders by security officers in the field.
3. Although two new procedures have been completed for the Security Control Center, there is still a need for comprehensive policies and procedures to be developed.

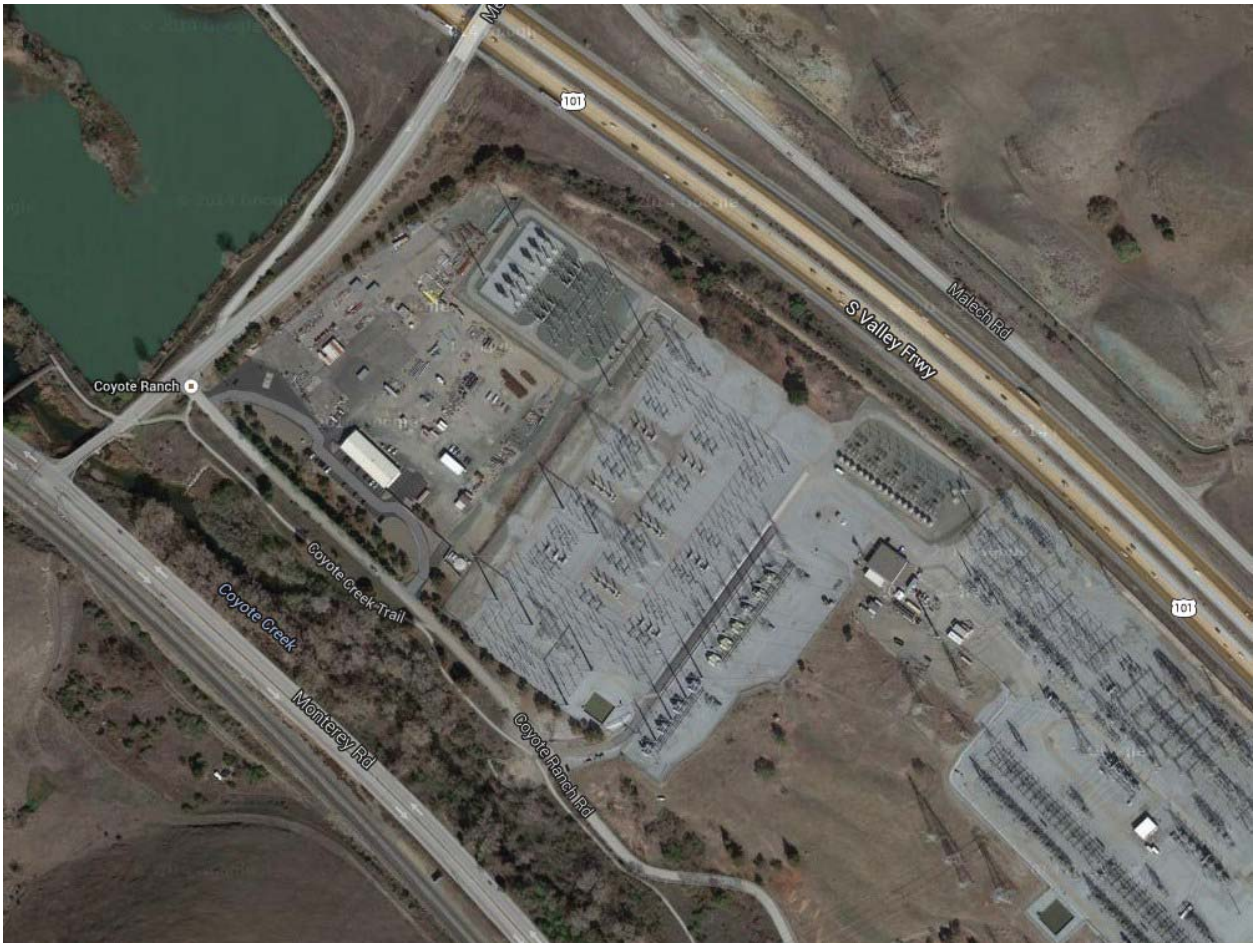
Action Plan Summary:

Cause Reference	Item	Description	Owner	Due Date	Status
Security breach	1	Secure Metcalf Substation fence	[redacted]	Immediate action	Complete
Security breach	2	Check all equipment for operational damage	[redacted]	Immediate action	Complete
Security breach	3	Security review of Metcalf Substation	[redacted]	Immediate action	Complete
Security breach	4	Increase Security officer presence on site	[redacted]	Immediate action	Complete
Security breach	5	Increase [redacted] lighting onsite	[redacted]	Immediate action	Complete
Security breach	6	Install [redacted] camera systems [redacted] sites to enhance security. Metcalf system has been installed	[redacted]	10/2/2014	Complete
Security breach	7	Vendor Replacement: Replace [redacted] with a vendor capable of establishing [redacted] of security officer movement.	[redacted]	11/15/2014	Complete
Security breach	8	Vendor Replacement: Replace [redacted] Operations Center Operations [redacted] New [redacted] addresses increased personnel and supervision	[redacted]	11/15/2014	Complete
Security breach	9	Re-establish patrols within Metcalf Substation	[redacted]	Immediate action	Complete
Post order compliance verification	10	Re-establish the Roving Supervisor position.	[redacted]	Immediate action	Complete
Security breach	11	Enhance [redacted] lighting	[redacted]	Immediate action	Complete
Lack of Policy & Procedure	12	Desk Procedures: Addressed alarm and incident response protocols for Operations Center personnel	[redacted]	9/10/2014	Complete
Lack of Policy & Procedure	13	Develop a comprehensive set of security policies and procedures for all work performed at the PG&E Security Control Center	[redacted]	Q2 2015	In Progress
Lack of Policy & Procedure	14	Implement [redacted] tests for all [redacted]	[redacted]	Immediate action	Complete
Lack of Policy & Procedure	15	Develop a comprehensive set of security policies and procedures for roles and responsibilities for contracted guard services.	[redacted]	Q4 2014	In Progress
Lack of Policy & Procedure	16	Develop a comprehensive set of security policies and procedures for training requirements and tracking process for Security Operators and contract security officers.	[redacted]	Q1 2015	In Progress

Cause Reference	Item	Description	Owner	Due Date	Status
Lack of Policy & Procedure	17	Develop a comprehensive set of security policies and procedures for Maintenance procedure(s) for all components of the security systems at [redacted]	[redacted]	Q2 2015	In Progress
Lack of Policy & Procedure	18	Develop a roles and responsibilities document for SCC PG&E Manager.	[redacted]	Q4 2014	In Progress
Lack of Policy & Procedure	19	Develop and document a process to prioritize, fund, implement and track recommendations from security evaluations.	[redacted]	Q4 2014	In Progress
Lack of Training	20	Trained Security Center Operators on Revised Alarm/Incident and [redacted] response protocols	[redacted]	9/12/2014	Complete
Lack of Training	21	Develop and implement a robust training program for Security Operators to ensure that alarms are responded to effectively.	[redacted]	Q1 2015	In Progress
Lack of Policy & Procedure	22	Implement the use of human performance tools in the SCC operations.	[redacted]	Q2 2015	Open
Timely maintenance of security systems	23	Transition the management of remote security systems from LOB's to CSD. This includes maintenance, repairs and capital replacement which will require an annual budget.	[redacted]	Q4 2015	In Progress
Maintain auditable review data	24	Implement a [redacted] logging system at the SCC.	[redacted]	Q1 2015	In Progress
Maintain auditable review data	25	Upgrade to a [redacted] logging system for the SCC.	[redacted]	Q1 2015	In progress
Alarm response	26	Accelerate the implementation of PSIM at SCC.	[redacted]	Q3 2015	In Progress
Security operator availability for shift coverage and training	27	Evaluate staffing levels of Security Operators and PG&E supervisor against workload at the SCC.	[redacted]	Q4 2014	In Progress
Efficiency / cost analysis	28	Evaluate the effectiveness of using a hybrid staff of contractor and PG&E employees at the SCC.	[redacted]	Q4 2014	In Progress
Document accessibility	29	Link procedure for "Alarm Response for [redacted] (currently an attachment to RISK-1001P-04) to RISK-1001P-05 with clear direction to use it.	[redacted]	Q1 2015	In Progress
GCC notification of security events	30	Tailboard Substation employees on the requirements in TD-3463P-01 to notify the Control Center of any security breach.	[redacted]	Q1 2015	Open
Alternate control center reliability	31	Verify all electrical systems required for operation of the alternate security control center in [redacted]	[redacted]	Q4 2014	Open

Cause Reference	Item	Description	Owner	Due Date	Status
New Control Center Facility	32	Work with Corporate Real Estate to acquire space for relocation of the PG&E Security Control Center	[redacted]	Q4 2015	Open
Lack of Policy & Procedure	33	Emergency Activation Planning: • Develop an emergency activation plan for the alternate security control center in [redacted] • Train the responsible security staff on the emergency activation plan. • Perform periodic relocation drills to ensure functionality of the plan and emergency preparedness.	[redacted]	Q1 2015	Open
Funding Priorities	34	Revise internal budgeting process to provide transparency and alignment between CSD's responsibilities and funding for security-related work	[redacted]	Q2 2015	In Progress
Contractor Management	35	Improve management of security contractors, including periodic meetings between CSD and vendors and performance dashboards	[redacted]	Q1 2015	In Progress

Attachment 1 – Metcalf Substation and General Construction Yard



Attachment 2 – GC Yard Burglary

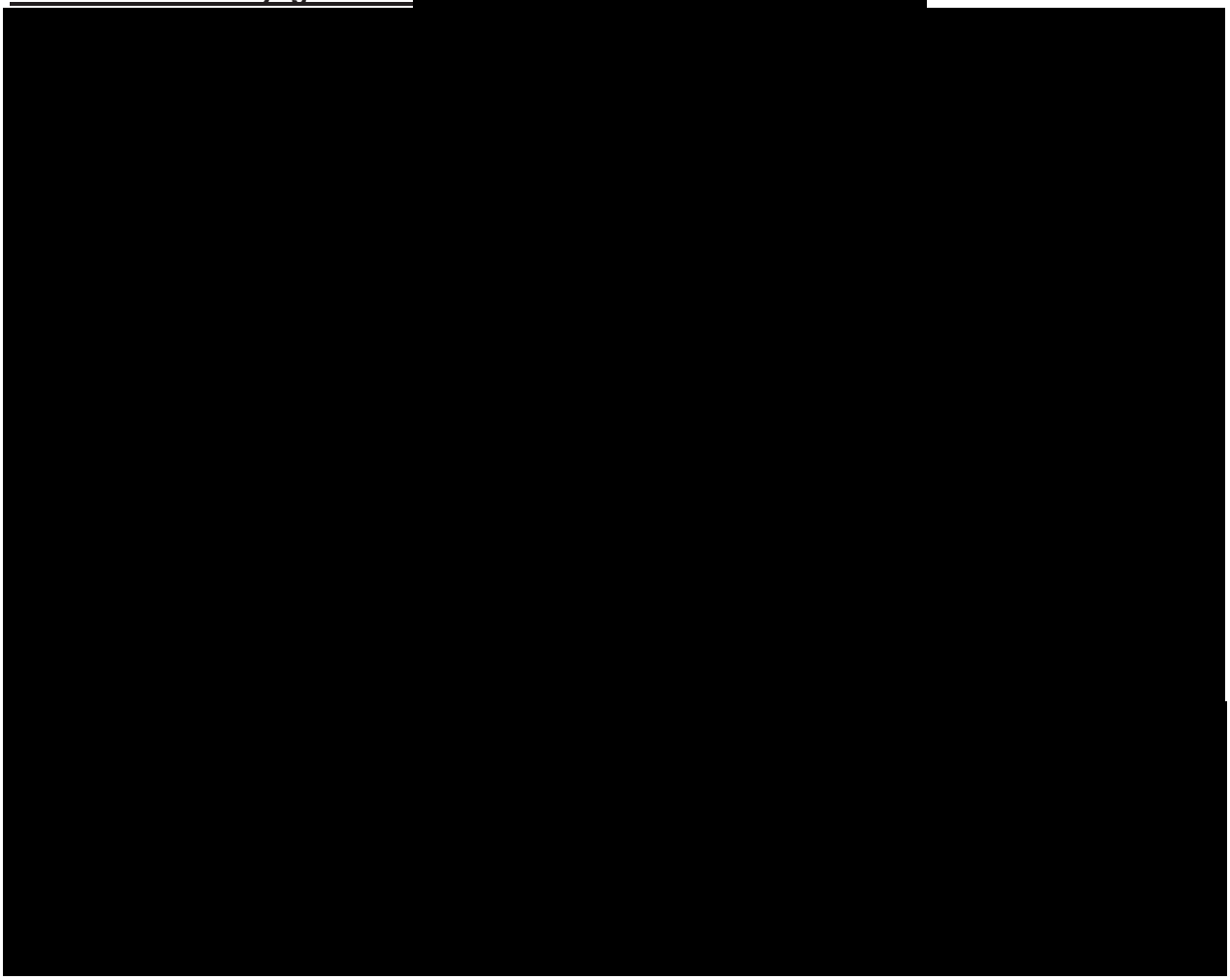
Attachment 3 – [redacted] Tower Which Captured Activity in GC Yard

Attachment 4 – [redacted] Cameras [redacted]

[redacted]

Attachment 5 – Camera [redacted] Alarm

Attachment 6 – Daylight View [redacted]



Attachment 7 – Fence Cut in Relation [redacted] -

Attachment 8 – [redacted]

Attachment 9 – [redacted] Coordination Procedures:

[redacted]

[redacted]

Attachment [redacted] Incident Response

[redacted]

[redacted]

[redacted]

Attachment 11 – Chronological Order of Event:

Per investigative and internal review –

At 2210, 2212, and 2252 hours, August, 26, 2014, alarms were triggered in the GC (General Construction) yard adjacent to Metcalf Substation. The GC yard security is monitored by [redacted] camera security system, a wholly separate vendor with no interconnectivity of alarms to FSCC [redacted] SO receives [redacted] alarm activation caused by people or material movement. [redacted] SO contacts [redacted] officer who confirms [redacted] are present at Metcalf. [redacted] Operator is informed on-site [redacted] security [redacted] on patrol. No specific additional actions are taken by [redacted] security [redacted] due to [redacted] SO's call. No further action taken by [redacted] operator [redacted] Alarm is logged as caused by shifting material and False.

At 2349 hours [redacted] camera security system receives alarm from GC yard, alarm is logged as no off-normal activity observed and false.

At 0202 hours August, 27, 2014 Alarm received at [redacted] SCC, [redacted] in Alarm / Metcalf Sub Fence Zone [redacted]

0203 [redacted] SCC receives an alarm from substation [redacted] Zone [redacted]

0204 [redacted] SO [redacted] No activity observed. Alarm cleared from alarm page. [redacted]

0209 hours –0218 hours [redacted] SO monitors other incoming [redacted] alarms [redacted]

0218 hours Second alarm received at [redacted] SCC: [redacted] in Alarm / Metcalf Sub Fence Zone [redacted] [redacted] SO [redacted] of Camera [redacted] No activity observed. Alarm cleared from alarm page.

02[redacted] hours Third alarm received at [redacted] SCC: [redacted] Alarm / Metcalf Sub Fence Zone [redacted]

02[redacted] hours Fourth alarm received at [redacted] SCC: [redacted] Alarm / Metcalf Sub Fence Zone [redacted]

02[redacted] hours Fifth alarm received at [redacted] SCC: [redacted] Alarm / Metcalf Sub Fence Zone [redacted]

02[redacted] hours Sixth alarm received at [redacted] SCC: [redacted] Alarm / Metcalf Sub Fence Zone [redacted]

02[redacted] hours Seventh alarm received at [redacted] SCC: [redacted] in Alarm / Metcalf Sub Fence Zone [redacted]

02[redacted] hours Eighth alarm received at [redacted] SCC: [redacted] in Alarm / Metcalf Sub Fence Zone [redacted]

02[redacted] hours [redacted] No activity observed. [redacted]

02[redacted] hours Ninth alarm received at [redacted] SCC: [redacted] in Alarm / Metcalf Sub Fence Zone [redacted]

02[redacted] hours Tenth alarm received at [redacted] SCC: [redacted] in Alarm / Metcalf Sub Fence Zone [redacted]

02[redacted] – 02[redacted] hours [redacted] camera security system (monitoring GC yard) [redacted] Alarm. [redacted] is observed having apparently tripped the alarm. No other activity seen. Alarm is logged as Alarm caused by shifting material" Alarm Resolution [redacted]

0600 hours A Substation Construction foreman sees the cut in the fence and notifies his supervisor.

0713 hours The Construction Supervisor reports the [redacted] breach to [redacted] Security instructs Supervisor to call Santa Clara County Sherriff's Office. SCCSO responds to the site at approximately 0730 hours.

1052 hours Substation Maintenance Electrician arriving at Metcalf Substation and finding Sherriff's Department on scene notifies GCC of their presence and security breach in fence.

Attachment 12 - Security Officer [redacted]

- **The [redacted] the night of August 26-27th and any changes that may have occurred in the contract language after the incident or after August 27th, 2014.**
  - **[redacted]**
    - **[redacted] originated in March 2014 by - [redacted]**
    - **[redacted] has been managed fiscally by [redacted]**
    - **[redacted] was written to include [redacted] corporate security request was to [redacted]**
    - **Guard Service schedule since this request is as follows; [redacted] guards 24 hrs [redacted]**
    - **Specific conditions to this purchase order include;**

- **2.0 Standards of conducts including specifically sections 2.1 including but not limited to Reporting to PG&E Corporate Security on all security issues and Respond to emergency situations to ensure proper handling of the incident**
- **4.0 Training Requirements including specifically sections 4.1.2.2 New officers will be [redacted] trained as follows, as applicable to the facility location: Walk-through facility briefing on and observing all applicable areas, Read the Post Orders**
- **7.4 Field Duties and Responsibilities including specifically sections 7.4.1.1Respond to all alarm conditions and any other indications of suspicious or emergency activities, 7.4.1.2 Perform thorough inspection of fence line and building perimeters for breach or break-ins, 7.4.1.3 Immediately report to the site contact evidence of materials stolen or in the process of being taken under suspect conditions, 7.4.1.8 Respond to suspicious and emergency related incidents, and provide detailed reports on theft, damage and/or emergency response, 9.8 Background Check Requirements 9.8.1 and subsection (i) and (ii)**
  - **Site Locations, Contacts and Guard Schedule are represented on Attachment 2-Site Locations as a part of the purchase order (specific duties would have been presented to resolute from the Post Orders via Corporate Security)**

On the afternoon of August 27th communications were presented to [redacted] that additional manpower was being placed immediately at Metcalf to increase the visibility of security which includes [redacted]

Attachment 13 - Post Orders In Effect at Time of Incident

INTERIM SECURITY OFFICER POST ORDERS
METCALF SUBSTATION INCIDENT

In response to an incident at the Metcalf Substation, physical security is being increased at other substations at the direction of Corporate Security. These post orders are developed to cover the patrol responsibilities at various locations. [redacted]

[redacted]

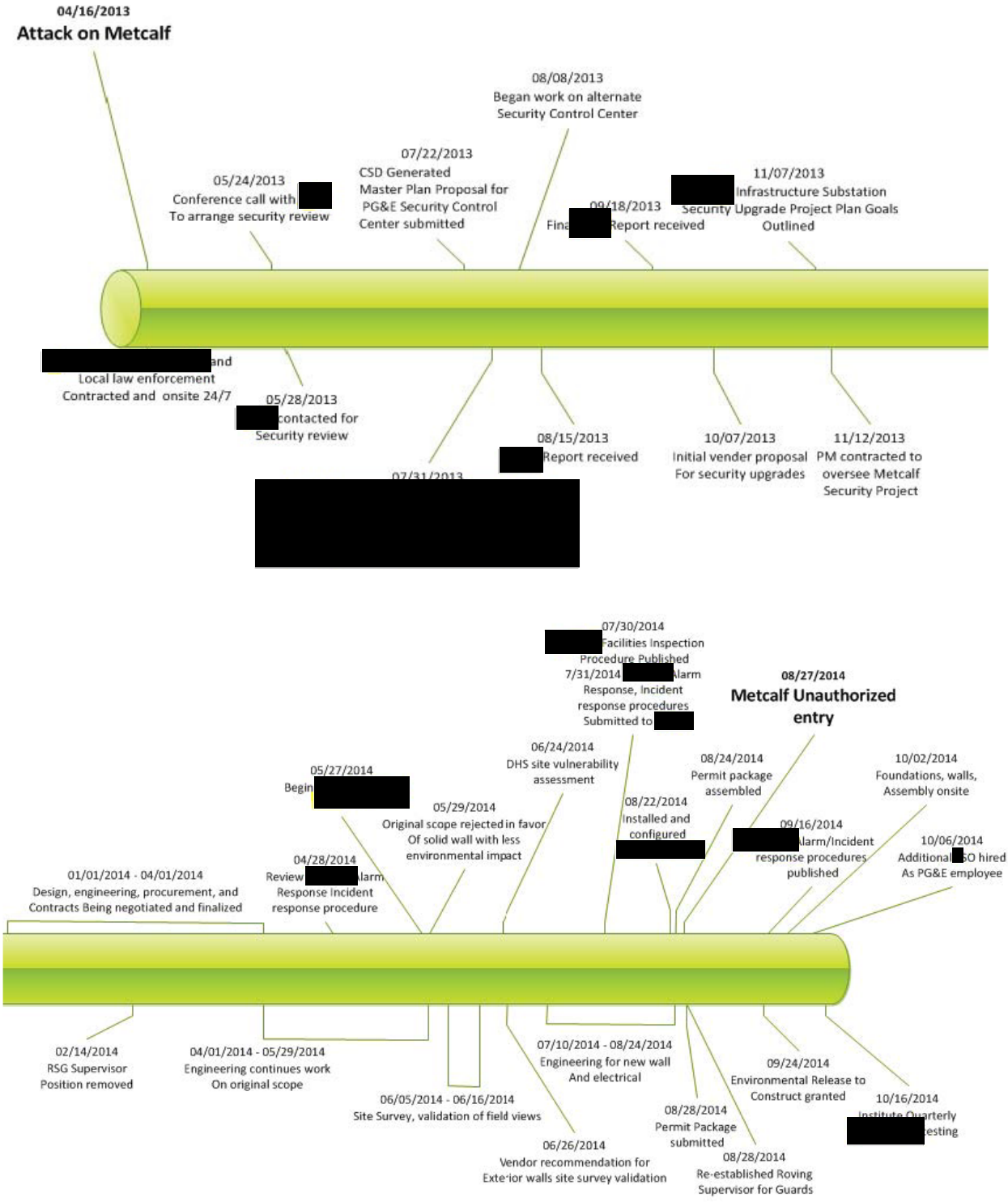
Attachment 14 – Summary of Actions Following the April 2013 Event

4/13	Contracted with local law enforcement to provide LE security for Metcalf and additional Substations. Contract continued [redacted]
4/13	Contracted with Private Security Company to provide 24/7 security officer coverage. - Ongoing
4/13	Installed [redacted] lighting [redacted]
4/13	Installed temporary fencing
5/13	Contracted with [redacted] to conduct a Vulnerability Assessment and Protection Options Study for Pacific Gas & Electric - [redacted]
5/13	Contracted with [redacted] to evaluate the transmission system by applying a Vulnerability Assessment Tool which scored vulnerability within PG&E's Transmission System
5/13	Reviewed [redacted] and receive a proposal to apply the system at Metcalf.
5/13	Contracted with [redacted] to review and provide recommendations PG&E's Physical Security Control System and [redacted] Security Control Center.
6/13	Law Enforcement agencies completed tours of [redacted] by Corporate Security. Latitude and longitude maps were issued to law enforcement [redacted] units and they were requested to provide [redacted] patrol when available.
7/13	Tailboards were developed and distributed to all major substations. [redacted] the facilities were given personal tailboards by Corporate Security investigators. During these tailboards topics of Metcalf, SAR reporting, and information on securing their facilities were discussed.
8/13	Received [redacted] Vulnerability Assessment and Protection Options Study
8/13	Received [redacted] evaluation of the transmission system based on the Vulnerability Assessment Tool which scored Substation vulnerability within PG&E's Transmission System.
8/13	Received approved permits and removed vegetation surrounding Metcalf
9/13	Received [redacted] report and recommendations for Physical Security Control System and [redacted] Security Control Center.
9/13	Initiated an internal training program which included suspicious activity reporting and awareness. The project team is composed of Corporate Security investigators and members of the PG&E Academy who developed Web-based training in securing our facilities and reporting suspicious incidents. CORP-9050 WBT
10/13	Released a Request for Proposal (RFP) for Physical Security Information Management (PSIM) to improve information management at [redacted] Security Control Center. Software solution (Physical Security Incident Management tool) will enable prioritization of alarms and enhance security response to incidents.

10/13	Improvements were made on the "Suspicious Activity Reporting" system in Corporate Security. A company mailbox was set up at SAR@pge.com system was developed to e-mail suspicious activity.
11/13	In conjunction with the Department of Homeland Security, FERC, NERC and the FBI, PG&E participated in an industry and law enforcement information sharing campaign in each of the 10 FEMA jurisdictions.
11/13	Initiated a contract for security improvements with [redacted] for the Metcalf Security Improvement Project
11/13	Contracted a Project Manager to coordinate the Metcalf improvement project
12/13	Received a Security Upgrade Design & Build Proposal from [redacted] for Metcalf Substation
1/14	Metcalf Improvement Project initiated: Internal tracking of physical and technological changes occurring at the substation. Project is projected for completion by end of Q1 2015
2/14	Received responses for the PSIM Request for Proposal
3/14	Contracted a procedure writer to formalize existing policies and procedures associated with the PG&E security system.
3/14	Conducted an assessment and test of current security systems at Metcalf
4/14	On the anniversary of the Metcalf event, PG&E announced a $250,000 reward for information leading to the arrest of responsible individuals
4/13	Additional camera added for Metcalf Substation
4/14	Worked with local law enforcement to provide enhanced security awareness on the anniversary of the Metcalf event
4/14	Completed Review of PSIM RFP submissions.
6/14	Contracted with [redacted] to evaluate and provide recommendations for processes and procedures at [redacted] Security Control.
6/14	Department of Homeland Security (DHS) performed a Site Vulnerability Assessment in coordination with PG&E Corporate Security and [redacted]
7/14	Posted job openings for [redacted] additional security operator positions at [redacted] Security Control
8/14	Received SVA from [redacted]
8/14	Performed on site post order training with security personnel at Metcalf
9/14	Enhance perimeter lighting of [redacted] locations with additional [redacted] lighting
9/14	Permit received on 9/22/2014 with flood zone contingencies - Construction underway on 2500' of the physical wall to be constructed outside identified flood zone – foundations underway (first wall expected to be installed week of Oct 12th)
9/14	Briefed alarm and incident response protocols for [redacted] operators and trained [redacted] Security Operators on revised Alarm/Incident and 3rd Party Response Protocols
9/14	Published Utility Procedure: Risk -1001P-05 [redacted] Security Control Center Alarm

	Response Procedure
9/14	Published Utility Procedure: Risk -1001P-04 [redacted] Security Control Center incident Response Procedure
10/14	Installed [redacted] Cameras at Metcalf Substation
10/14	Performed security review and [redacted] testing at Metcalf and [redacted] Substations
11/14	Replaced [redacted] guard [redacted] and [redacted] Security Operations [redacted]

Attachment 15 – Time Line



Attachment 16 – Response to Access Control Alarms (6-21-2012)

SUBJECT: Access Control Alarms

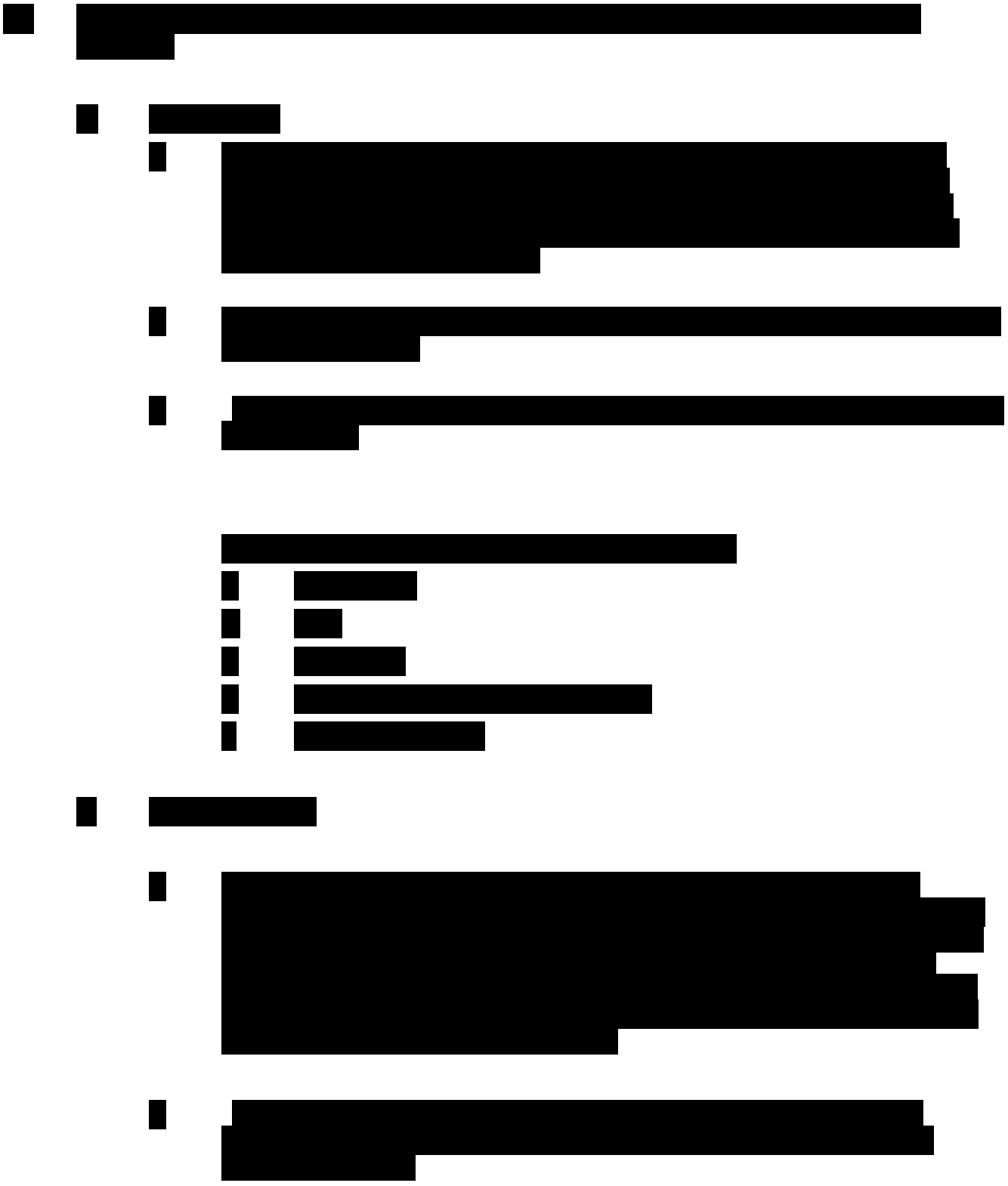
TITLE: Response to Access Control Alarms

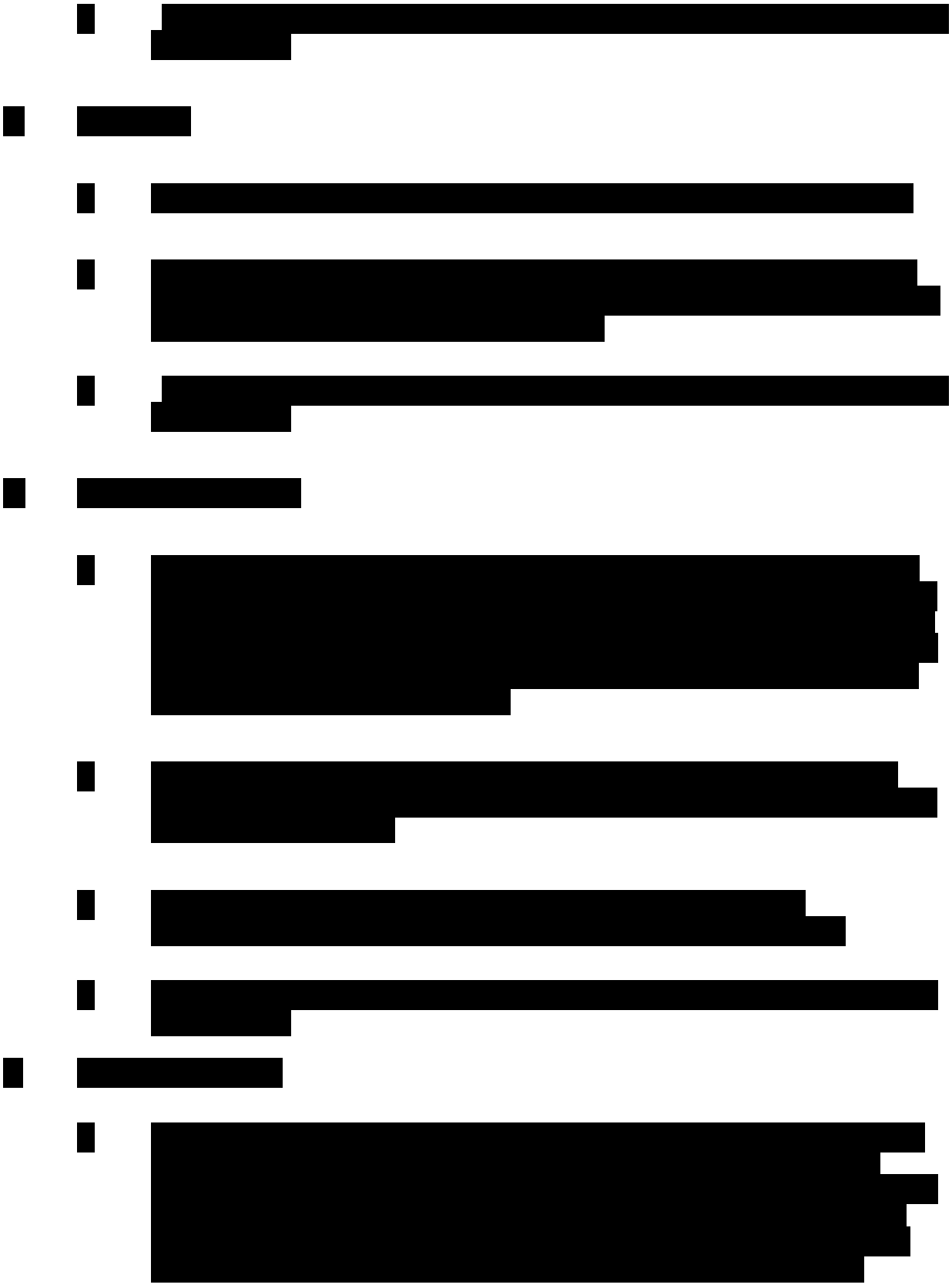
EFFECTIVE: March 16, 2009

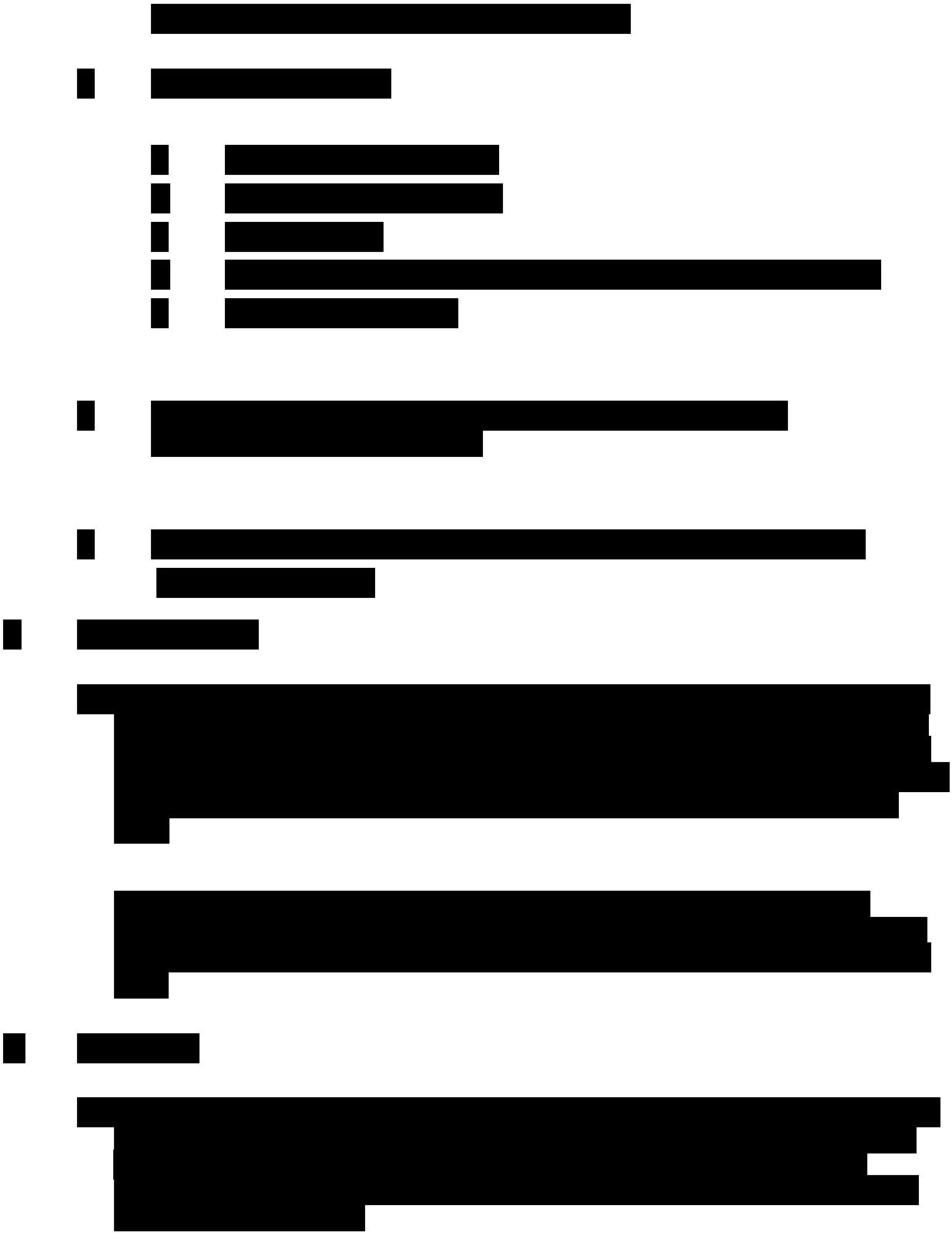
UPDATED: June 21, 2012

[redacted]

[redacted]







[redacted]

Attachment 17 – Excerpt From [redacted]

- [redacted] originated in March 2014
  - Specific conditions to this [redacted] include but are not limited to;
    - 2.1 Standards of conducts including specifically sections 2.5 including but not limited to (h) Continually develop and upgrade the training program for the Security Officers in accordance with the Bureau of Security and Investigative Services (BSIS) California Code of Regulations effective 8/2005, (m) Ensure that no officer works the console desk without proper training (i.e. knowledge of fire alarm system), (t) Respond to emergency situations to ensure proper handling of the incident. Be prepared to assume command of the emergency if the situation calls for such action, (u) Support PG&E's emergency response procedures by assisting in security control, (v) Ensure that all notification procedures are followed regarding security incidents at PG&E facilities
    - 4.1 Training Requirements including specifically sections 4.2.1The Facility Manager, along with the support of the Supervising Lieutenant, has the responsibility of ensuring that training of new hires and existing employees on staff is completed and provided to Corporate Security. It is important that the trainee be trained on the duties of the position they are assigned, 4.2.2 New officers will be minimally trained as follows, as applicable to the facility location: Walk-through facility briefing on and observing all applicable areas, Read the Post Orders, Train in detail all procedures, then the new Security Officer will demonstrate to the instructor knowledge and comprehension of the procedures, Retrain all areas not fully understood by the new Security Officer, Complete a post-training checklist, Complete twenty-four (24)hours of training on facility system before manning a post solo
    - 6.1 Post Orders including specifically section 6.2 Purpose-Security Officers shall perfor [redacted] of PG&E service territory which include, but are not limited and may change during the contract period of performance, to the following locations:(Area six

[redacted]