Application No.:
Exhibit No.: SCE-07, Vol. 04
Witness: D. Daigler

SOUTHERN CALIFORNIA EDISON®

An *EDISON INTERNATIONAL*® Company

(U 338-E)

2015 General Rate Case

Safety, Security, & Compliance (SS&C) Volume 4 – Corporate Security and Business Resiliency

Before the

Public Utilities Commission of the State of California

Rosemead, California
November 2013

SCE-07: Safety, Security, & Compliance
Volume 04 – Corporate Security and Business Resiliency

Table Of Contents

SCE-07: Safety, Security, & Compliance
Volume 04 – Corporate Security and Business Resiliency

Table Of Contents (Continued)

SCE-07: Safety, Security, & Compliance
Volume 04 – Corporate Security and Business Resiliency

Table Of Contents (Continued)

SCE-07: Safety, Security, & Compliance
Volume 04 – Corporate Security and Business Resiliency

Table Of Contents (Continued)

SCE-07: Safety, Security, & Compliance
Volume 04 – Corporate Security and Business Resiliency

Table Of Contents (Continued)

SCE-07: Safety, Security, & Compliance
Volume 04 – Corporate Security and Business Resiliency

Table Of Contents (Continued)

SCE-07: Safety, Security, & Compliance
Volume 04 – Corporate Security and Business Resiliency

List Of Figures

SCE-07: Safety, Security, & Compliance
Volume 04 – Corporate Security and Business Resiliency

List Of Tables

List Of Tables (Continued)

I.

OVERVIEW OF CORPORATE SECURITY AND BUSINESS RESILIENCY

A. Overview and Summary of Test Year Forecast

This volume addresses the duties and test year expenses of the Corporate Security and Business Resiliency Departments. Prior to 2013, these activities were managed in a single department. In late 2012, Business Resiliency was separated from Corporate Security and designated as an independent department. Both departments continue to record labor and non-labor expenses to the same 920/921 A&G FERC account but, to more accurately forecast expenses, the costs of each department are presented individually below. In addition, Corporate Security records outside vendor costs for background checks to FERC Account 923.

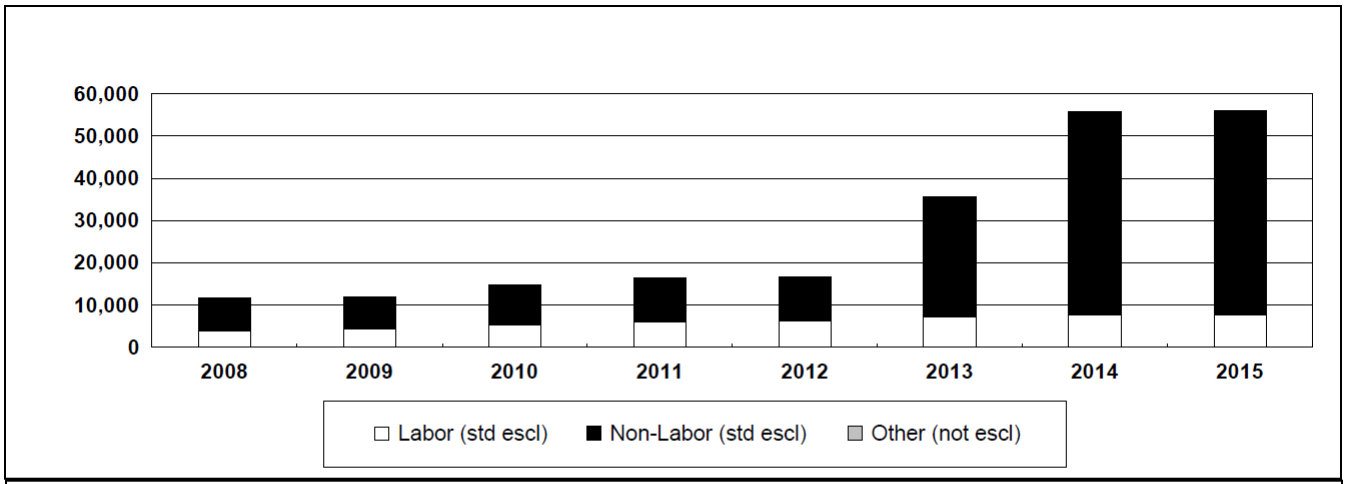
For 2015, the Corporate Security and Business Resiliency Departments forecast O&M expenses of $56.099 million for FERC Accounts 920/921, and $0.151 million for FERC Account 923, an increase of $39.629 million and $0.028 million, respectively, over 2012 recorded costs. As described below, the increase is needed for significantly expanded security activities to reasonably address security risks, to fulfill regulatory mandates, and for improved emergency response planning and preparedness. A summary of the departments' 2015 O&M expense forecasts is provided in Table I-1 below.

Table I-1
Summary of Corporate Security and Business Resiliency
2015 Test Year O&M Expense
(Constant 2012 $000)

Line No.	Department/FERC Account	2012 Recorded Adjusted	2015 Test Year Forecast
1	Corporate Security 920/921	14,646	52,099
2	Business Resiliency 920/921	1,824	4,000
3	Total 920/921 (Line 1 + Line 2)	16,470	56,099
4	Corporate Security 923	123	151
5	Total Corporate Security and Business Resiliency (Line 3 + Line 4)	16,593	56,250

Figure I-1 below provides the 2008-2012 recorded/adjusted and 2015 forecast O&M expenses for Accounts 920/921.

Figure I-1
Corporate Security and Business Resiliency
FERC Accounts 920/921
2008-2015 Adjusted/Recorded and Forecast Expenses*
(Constant 2012 $000s)



	2008	2009	2010	2011	2012	2013	2014	2015
Labor	3,768	4,141	5,127	5,838	6,155	7,025	7,605	7,605
Non-Labor	7,922	7,790	9,474	10,542	10,315	28,467	48,084	48,494
Other	0	0	0	0	0	0	0	0
Total	**11,690**	**11,931**	**14,601**	**16,380**	**16,470**	**35,492**	**55,689**	**56,099**

Forecast

*Due to rounding, totals in figure may not tie to other figures in this testimony volume.

Corporate Security is also estimating $137.881 million in capital investments for 2013-2017, which are needed for SCE to comply with more stringent infrastructure protection regulations expected to become effective in 2015 (the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards (Standards)), to improve workplace security and grid reliability protections, and to maintain adequate security monitoring of SCE facilities.

B. Key Drivers of O&M Expense Increase

The 2015 O&M forecast reflects the continuation of well-established security and business resiliency functions, significantly influenced by four issues. The first is the need to improve workplace security and grid reliability protections. Recent violent attacks on human life (the 2013 Boston Marathon bombings), apparent acts of sabotage (the 2013 PG&E Metcalf substation incident), and incidents of workplace violence (the 2011 Rivergrade shooting incident) highlight the need to address

potential threats through a more robust prevention, deterrence, interdiction, and mitigation approach.[1] SCE will achieve this through the heightened security measures discussed in Chapter II. Another recent event, the wind storm of November 2011, caused SCE to reassess its practices and procedures for emergency preparedness. As discussed in Chapter III, Business Resiliency is taking significant steps to improve SCE's ability to prepare for and respond to a variety of emergencies. A third driver is an imminent regulatory mandate that will require significant additions to the protections currently in place for critical infrastructure, specifically in the area of NERC-regulated cyber asset protection. The fourth cost driver is the need to upgrade SCE's security infrastructure to address functionality and reliability risks created by the age or obsolescence of security equipment.

[1] *See* workpapers entitled "CNN: Boston Marathon Terror Attack Fast Facts," "CBS: Vandalism at San Jose PG&E Substation Called Sabotage," and "SCE Press Release: Fatal Shootings at Southern California Edison Irwindale Facility."

II.

CORPORATE SECURITY

A. Overview and Summary of Test Year Forecast

Corporate Security is responsible for the protection of SCE employees, visitors, customers, and company assets. For 2015, Corporate Security forecasts $52.098 million and $0.151 million in O&M expenses for FERC Accounts 920/921 and 923, respectively. Corporate Security also forecasts $137.827 million for 2013-2017 in required capital improvement to support SCE's operations.

Corporate Security's forecast reflects an increase in O&M expenses of $37.329 million over 2012 recorded expenses. The primary drivers for the increase are the need to:

- Implement workplace security improvements to protect grid reliability, which were identified by Facility Security Assessments and are based on: (1) the criticality of the facility to the Bulk Electric System (BES), (2) employee and visitor populations and traffic, and (3) crime rates in a given locale.
- Commission and deploy a new Edison Security Operations Center (ESOC) capable of supporting improved access control monitoring, alarm event management, and physical security of cyber systems (as defined by NERC CIP v5 Standards).
- Properly maintain and repair new security systems, address degradation of existing systems, ensure adequate employee badge stock, and license necessary security software and related security system equipment.
- Install the systems and processes needed to comply with NERC CIP v5 requirements for the protection of cyber assets critical to operating the BES.[2]
- Install security and access control systems at SCE facilities that currently do not have an existing security system or centrally managed access controls.
- Upgrade elements of existing security systems at electrical facilities and business locations that create unacceptable risk due to obsolescence, such as systems that are beyond manufacturer recommended capacity and/or service life.

---

[2] Please see Mr. Pespisa's testimony in Exhibit SCE-09 for a discussion of the background of NERC CIP Standards, the upcoming NERC CIP v.5 Standards, and their operational impacts on SCE. The implementation of the physical security aspects of the NERC CIP v.5 Standards delegated to Corporate Security are discussed in this volume.

- Upgrade the electronic security of the Corporate Security applications infrastructure to improve cyber security protection of the physical security computing environment, reduce the risk of cyber threats and impacts on security operations, and comply with the NERC CIP-006 Standard.
- Continue video surveillance and intrusion detection improvements to the perimeters of A-Bank substations that do not have security systems that monitor security perimeters, building access, or gate access.

B. Summary of Activities

Corporate Security is part of SCE's Safety, Security, and Compliance (SS&C) Operating Unit (OU). The primary responsibility of Corporate Security is to support the reliability of the electrical system by protecting SCE and its assets—employees, facilities, and infrastructure—and the public from threats, disruptions, and security vulnerabilities on behalf of our customers. The operational continuity of the SCE electric infrastructure is critical to the vitality of Southern California, and to the health, safety, and security of our five million customers, which include military and police facilities, fire service facilities, hospitals, day care centers, critical care facilities, public safety agencies, small business owners, and individuals with special needs. Corporate Security plays a vital role in SCE's ability to provide safe, reliable, and affordable electric service upon which all our customers rely and which SCE is obligated to provide.

Corporate Security is responsible for preventing and deterring vandalism, theft, and property damage to SCE assets, and preventing unauthorized access to SCE's critical assets, control systems, equipment, and information. We use a variety of physical security controls and strategies to identify possible incidents, log incident information, and report attempted malicious acts. Obstacles such as fences, barriers, and walls are used to stop or frustrate intruders and delay more determined ones. Access control systems–such as gates, doors, and locks–restrict access to controlled areas to only those with appropriate authorization and identification. Alarms, lighting, guards, and video surveillance detection systems provide notification to Corporate Security personnel of potential security breaches or policy violations, while intrusion detection and response systems help identify, respond to, investigate, and track all incidents. Background investigations are performed to identify and authenticate every candidate for employment prior to hire. Employees requiring access to NERC CIP sites are subject to additional scrutiny in the form of Personnel Risk Assessments (PRAs).

We collaborate with all of SCE's OUs as needed or requested to identify, mitigate, and respond to threats to its operations and the well-being of employees, customers, and the public. We provide subject matter expertise for securing and monitoring SCE facilities to minimize disruptions to business operations that can affect the safe and reliable delivery of power to SCE customers.

As part of our business practices, we maintain working partnerships with federal, state, and local law enforcement agencies, public safety agencies, and regulators. These partnerships allow SCE to quickly and accurately provide and receive essential information to protect the critical infrastructure vital to SCE's ability to provide safe and reliable power, effectively secure and protect transmission and distribution lines, and provide faster and more efficient responses to emergencies ranging from down wires to terrorist threats. Partnerships include local police, sheriffs, fire departments, the Federal Bureau of Investigation, and the Department of Homeland Security.

Corporate Security is comprised of three functional areas: (1) Physical Security Systems & Controls, (2) Asset Protection & Security, and (3) Operational Services. An overview of the activities of these areas is provided below.

1. Physical Security System & Controls

The Physical Security Systems & Controls group is responsible for the design and deployment of all physical security systems at SCE, as well as the technology platforms for the operation of the Central Alarm Station (CAS) and Edison Security Operations Center (ESOC).[3] The group manages all physical security systems, oversees the employee badging office, and coordinates security technology system changes and solutions.

Physical Security Systems & Controls manages the granting and revocation of physical access privileges to facilities, based on organizational needs and corporate policies and procedures. The badging office issues electronically encoded badges used to identify the badge holder as an employee, visitor, vendor, or contingent worker. Because identity management of personnel is an important practice in any security program,[4] each badge is uniquely encoded and interfaces electronically with security control systems to provide its user access to only those SCE facilities that have been specifically authorized in the systems for that user. Access to facilities and buildings is based on this corporate

---

[3] As discussed in Chapter II, Section C.2, below, the ESOC will replace the CAS.

[4] *See*, *e.g.*, ASIS International, *Security Management Standard: Physical Asset Protection*, page 40, B.5 Physical Entry and Access Control (ANSI/ASIS PAP.2-2012). This copyrighted publication is not included as a workpaper as ASIS International prohibits the reproduction and dissemination of the document.

badging system, which controls remote locking and unlocking of facility access points through the alarm system. The group consists of our Physical Security Protection Systems team and NERC CIP Process & Controls team, which are discussed in more detail below.

a) Physical Security Protection Systems

The Physical Security Protection Systems team is responsible for designing, deploying, documenting, and maintaining physical security protection systems across SCE. This includes the integrated system of infrastructure components needed for centralized monitoring and response to alarm and security incidents across the broad range of SCE facilities. The group is also responsible for managing the physical access and controls systems required by the NERC CIP Standards.

The NERC CIP Standards currently define "Critical Cyber Assets" (CCAs) as those cyber assets that are closely related to the reliable operation of the BES. The Standards specify very restrictive security controls that must be maintained around these CCAs, including rigorously defined physical security perimeters (six-walled security containment areas, also called PSPs) that must be erected around all CCAs and monitored at all times. Any access or attempted access to CCAs must be continuously logged and reviewed without gaps.

The Standards require formal procedures and detailed documentation for system configuration and testing, as well as preventative maintenance. These include any repairs or modification of the PSPs, the access control and monitoring systems that protect them, and the CCAs contained within the systems. Authorized entries into PSPs, and the logging of each such entry, is managed by a computerized identity verification system and computer-controlled locking devices. The Physical Security Protection Systems team administers the access control system and is responsible for complying with NERC requirements governing the verification, provisioning,[5] and revocation of access to PSPs and CCAs. The group is also responsible for:

- Installing barrier systems to protect property lines, critical assets, and operating equipment;
- Intrusion detection and video surveillance of facility perimeters, access points, and critical assets;

[5] "Provisioning" is the process of providing users with access to data and technology resources where users are given access to facilities, data repositories, systems, and/or applications.

- Managing the maintenance of technology platforms and tools for the ESOC; and
- With Corporate Real Estate and Corporate Security Asset Protection, hardening property lines, fence lines, doors, and critical assets.

b) NERC CIP Process & Controls

The NERC CIP Process & Controls Team manages the NERC CIP compliance requirements delegated to Corporate Security.[6] Corporate Security's NERC CIP responsibilities include the requirements related to physical access control (NERC CIP-006 Standard) and many of the requirements relating to personnel and training (NERC CIP-004 Standard). The group is responsible for developing and maintaining the SCE physical security plan required by NERC CIP-006 and the associated processes, procedures, and compliance evidence. The team supports annual vulnerability assessments and internal and external audits, and analyzes potential non-compliance events and gaps causing compliance risks.

Additionally, NERC CIP Standards require SCE to conduct annual vulnerability assessments of all NERC physical security perimeters and systems. The Standards require annual self-certifications that can only be made after extensive review of compliance evidence, along with an annual review and update of all compliance procedures and security plans. The Standards also require methodical management and documentation of changes to the security configurations and of all maintenance and testing of the security systems. These activities are required to comply with NERC CIP Standards and to secure the CCAs.

SCE currently has 35 NERC physical security perimeters that are monitored and managed by the NERC CIP Process & Controls team.[7] SCE is subject to compliance audits for conformance to the NERC CIP Standards governing PSPs.[8] In the past three years, the NERC CIP Process & Controls team has supported three WECC audits of the NERC CIP Standards. Each audit required months of preparation and coordination with other OUs, and included documentation updates,

---

6 Please see Mr. Pespisa's testimony in Exhibit SCE-09, Vol. 3: Regulatory Operations and Regulatory Policy & Affairs for a discussion of the NERC CIP Standards, including NERC CIP compliance functions delegated to other OUs and departments.

7 As discussed in Chapter II, Section F.4., the NERC CIP v.5 Standards are projected to increase the number of physical security perimeters requiring monitoring to over 140.

8 Although the audits are typically conducted by the Western Electricity Coordinating Council (WECC), NERC and the Federal Energy Regulatory Commission (FERC) can also enforce compliance with the NERC CIP Standards.

compilation of compliance evidence, verification and validation of physical security perimeter integrity, interviews, presentation of evidence, responses to data requests, analysis and remediation of issues, and post-audit process improvements.

2. Asset Protection & Security

The primary role of the Asset Protection & Security group is to protect employees and prevent crimes on SCE property. The group conducts criminal and civil investigations of security incidents and threats. The range of threats is broad and encompasses criminal activity, potential workplace violence, and threats to the electric system, such as vandalism, sabotage, and terrorism. Additional responsibilities include background investigations (employees, prospective employees, and contractors), providing security support services, and managing and escorting visitors. The group is further divided into the Investigative Services team and the Background Investigations & Security Services team, which are discussed in more detail below.

a) Investigative Services

The Investigative Services team includes Regional Special Agents (RSAs) and Facility Security Coordinators (FSCs). The team handles a variety of issues, including crimes of fraud against the company and/or customers, executive and workforce protection, theft or vandalism of employee or company property, and threat management (*e.g.*, public demonstrations and suspicious packages/mail).[9]

RSAs are assigned to specific portions of SCE's service area and are on call 24 hours a day, seven days a week, and 365 days a year (24/7/365). They conduct investigations of suspected criminal acts or threats against customers (such as property line disputes), SCE, or employees in coordination with federal and state law enforcement agencies, regulatory agencies, and other public safety officials. They advise grid operators, call centers, land managers, SCE Field Service Representatives, and other internal and external organizations on a variety of issues, including minimizing loss of assets, preventing sabotage to systems, avoiding delays in critical projects, thwarting threats to customers by employee imposters, preventing or identifying power theft, and preventing other crimes that can affect SCE operations or SCE's ability to provide electric service to customers. RSAs

[9] Examples of fraud on customers include incidents where individuals posing as SCE employees demand payment from customers. Examples of internal fraud include embezzlement, changing names on checks, and insider trading.

provide essential support to law enforcement agencies and prosecutors to bring cases to just conclusions, and provide SCE management with timely and objective assessments of the facts surrounding an event.

FSCs are deployed at SCE headquarters and other important SCE facilities, each having responsibility for a specific territory. FSCs attend to the physical security needs of facilities within their territory and oversee contract security officers at their respective locations. They also respond to overnight emergencies anywhere in their assigned service territory. FSCs document all security-related events for use in further investigations or in personnel or law enforcement actions. FSCs also support RSAs and local law enforcement as needed, and serve as liaisons between on-site management and operations, the Physical Security Systems & Controls group, and SCE Facility Management.

b) Background Investigations & Security Services

The Background Investigations & Security Services group is responsible for conducting all background investigations of potential employees and contract workers, in addition to new and recurring investigations for individuals requiring access to physical security perimeters and CCAs, which are governed by NERC CIP Standards. The group provides management oversight of the 287 contractor-provided security officers at 22 fixed posts throughout SCE, which includes contract management duties and managing any situations requiring extra security, such as on-demand security services.

On-demand security services involve the temporary deployment of security officers to protect employees, assets, customers, and the public, including during emergencies and power outages. The nature of on-demand service allows SCE to design specific deployment strategies to make the most effective and economical use of these services.[10] On-demand services are used to help prevent theft of SCE assets (*e.g.*, copper and other metals), protect company property during construction and maintenance projects, prevent trespassers on SCE property, and support planned and unplanned NERC CIP outages as explained in Chapter II, Section C.4. The Security Services team also manages the staffing of responses to physical security incidents.

3. Operational Services

The Operational Services group performs the business support functions for Corporate Security. The group is responsible for leading cross-functional project managers and teams in

[10] *See* workpaper entitled "Cost Effectiveness of Using On-Demand Security Officers."

coordinating various departmental projects, and for building partnerships with organizations and teams across SCE and external agencies. Operational Services provides reception and general administrative support, develops security-related processes and policies, and leads the development of the department's strategic initiatives, its one-to-five year strategic plan, and departmental goals.

The Operational Planning and Analysis team under Operational Services manages the Threat Management, Workplace Violence Prevention, and Workplace Security programs. The Workplace Security program includes the Workforce Protection and External Threats programs.

C. Drivers for Incremental O&M Expenses

Corporate Security is requesting an increase in O&M expenses for 2015 for enhanced security measures to improve workplace security and grid reliability protection, to staff the new ESOC, for the necessary maintenance and repair of security systems at NERC CIP and non-NERC CIP sites, and for on-demand security services for NERC CIP manual observations.

1. Workplace Security and Grid Reliability Protection Improvements

Protecting grid reliability and the electrical infrastructure supporting the grid as well as the safety and security of our employees, visitors, and customers at SCE facilities is a top priority. To improve workplace security and the protection of electric grid reliability, SCE is enhancing the skills and qualifications of our contract security officers, assigning security officers to locations currently lacking a security presence, and implementing a screening program at key facilities to prevent unauthorized weapons or materials from entering the workplace. SCE will enhance security measures at facilities that are critical to BES reliability (including grid control and data centers), engineering headquarters, customer-oriented facilities (such as call centers), and facilities that have the most numbers of employees and visitors.

a) Enhanced Security Measures

Some recent events have contributed to SCE's decision to address potential threats by a "harden the target" prevention, deterrence, interdiction, and mitigation approach. First, the 2013 Boston Marathon bombings highlight the terrorist tactic of individuals operating in small cells to create disruption, injury, and chaos. Second, the recent acts of apparent sabotage involving Pacific Gas & Electric (PG&E) highlight the vulnerability of electric system infrastructure, particularly substations. In April 2013, multiple rounds from an apparent assault weapon were fired into transformers at PG&E's Metcalf 500kV substation and adjacent telecommunications lines were cut, damaging transformers and

causing the release of hazardous materials. Third, in December 2011, a workplace shooting incident at SCE's Rivergrade facility resulted in three fatalities, and two others were wounded in the incident.

Additionally, SCE employees and executives have been confronted by activists and protestors who take issue with certain SCE business operations, such as the San Onofre Nuclear Generating Station (SONGS) and the Tehachapi Renewable Transmission Line Project (TRTP). These groups have interrupted meetings, blocked construction operations, and conducted protests at various SCE facilities and worksites. Finally, the findings and recommendations of Facility Security Assessments conducted in 2012 (discussed in Section b below), were also considered in the implementation of enhanced security measures.

The enhanced security measures also address one aspect of SCE's Workplace Improvement Plan (WIP), which was created in 2012 to further improve SCE's work environment. The WIP is comprised of four key components: (1) improving our management and leadership expertise and behaviors, (2) changing our organization structure and people, (3) listening to our employees and resolving issues, and (4) improving workplace security. Corporate Security is responsible for the last of the above WIP components – improving workplace security – and is focused on enhancing facility security and developing and implementing a Threat Management Team, Workplace Violence Prevention Program, and a Workplace Protection Program.[11]

To improve workplace security and the protection of grid reliability, SCE is implementing a new approach to the use of contract security officers. SCE is using three guard categories – armed, enhanced, and basic – to increase visibility (thereby impacting deterrence), mitigate losses, and provide for a faster and more robust response to security incidents. The decision as to what type of guards are appropriate at particular locations is based on a consideration of three factors: (1) the criticality of the facility operations to the electrical systems, (2) the number of employees assigned to the facility and the number of visitors to the facility, and (3) local crime rates.

Based on the these three factors, at certain locations SCE will use armed guards who have significantly greater training, skill sets, and expertise than basic security officers, including many who have military and/or law enforcement experience. These armed guards are assigned to locations where consideration of the factors makes this a prudent decision for improved safety and

[11] Please see Ms. Miller's testimony at Exhibit SCE-06, Vol. 1, for a discussion of the other three components of the WIP.

security. The deployment of armed guards is limited to positions where they are highly visible, such as perimeter gates and building entry points, to maximize deterrence.

Enhanced guards are unarmed but have more sophisticated training, experience, and decision making skills than basic security officers. Enhanced guards, who have a more professional appearance and present a greater deterrence, will be used at positions and locations within the SCE territory where consideration of the above-noted factors does not warrant the use of armed guards but does support the need for more experienced and trained guards. Basic security officers are deployed at the balance of locations where a presence is deemed prudent, but the combination of factors does not support the need for armed or enhanced guards.

SCE has endeavored to use a mix of armed, enhanced, and basic guards based on the risks presented with each facility, the potential for the greatest harm and impact, and the safety of the systems and people who operate them. Instead of a "one size fits all" approach, this mix is a balanced and considered strategy designed to achieve our goals efficiently and economically.

An additional component of the enhanced security measures is the implementation of a screening program to detect weapons and other unauthorized materials and prevent them from entering key facilities where they have the maximum potential to damage SCE's operations. Metal detectors and X-ray scanners provide a barrier to the entry of unauthorized weapons or materials and are features commonly used at facilities where an elevated level of security is desired, such as government buildings, airports, sports and entertainment venues, and court houses. The screening program consists of the installation of turnstiles with metal detection equipment, baggage X-ray scanners with conveyor belts at facility entrances, and parcel X-ray scanners at loading docks, all supported by armed security officers. Additionally, Parcel X-ray scanners will be added to mail rooms at these facilities and supported by trained mail room employees.

b) Facility Security Assessments

In 2012, Corporate Security conducted onsite Facility Security Assessments (FSAs) of office buildings, service centers, combined facilities, substations (switching centers), and warehouses to evaluate security operations, site-specific security measures, technology tools, security staffing, and security policies and procedures. The assessment was based on types of threats/risks, probability of threats/risks, and the effect on the asset if the risks occurred. The purpose of the FSAs was to identify issues and develop recommendations relating to SCE's security systems, policies, and procedures for protecting SCE's assets, personnel, and visitors as well as SCE's compliance with

applicable regulatory requirements. As a result of SCE's evaluation of the FSAs, SCE is implementing a number of necessary security enhancements. The testimony below discusses the O&M costs associated with the improvements while the capital expenditure impacts are addressed in Chapter II, Section F.2.

The FSAs were conducted by an external vendor, Corporate Risk Solutions, Inc. (CRSI),[12] with Corporate Security's active participation.[13] The FSAs were conducted in three phases. During Phase I, CRSI assessed SCE's eight largest facilities, 31 buildings, and approximately 45 percent of the workforce population. For Phase II, CRSI assessed a representative sample of 23 facilities, 55 buildings, and an additional 20 percent of the workforce. Phase III included an assessment by Corporate Security of seven facilities to obtain a representative sample of all remaining facility types.

Upon completion of the assessment, CRSI determined that all assessed facilities were vulnerable to identified risks and threats, some of which were unique to specific locations, and others that were common to all facilities. Although there were facilities that had implemented best practices (*e.g.*, emergency call boxes, collaboration between Corporate Security and contract security officers, signage to assist with pedestrian flow at multi-use facilities, and binders with photographs of restricted individuals), certain security program components needed immediate attention across all locations. These components included cameras (additional, replacement, or new), improved exterior perimeter lighting, vegetation control to minimize cover and concealment for intruders, door repair and maintenance, increased security guard staffing levels and training (to address safety, coverage levels, and security), and enhanced perimeter and building access controls. Improvements were also recommended from a corporate level, including overall security policy changes, enterprise training and awareness, and enterprise visitor management solutions. SCE reviewed CRSI's observations and recommendations and, after evaluating the most effective and economical means to address the identified issues, adopted some recommendations while declining others.

Based on the FSA recommendations, SCE has re-evaluated its strategy for the deployment of security guards and determined that it was necessary to increase and/or add security guard presence at our most important and/or vulnerable facilities. Facilities were examined based on the

---

[12] CRSI is an independent security consultant that does not sell security technology devices, serve as a system integrator, or provide security officer services. Therefore, their observations and recommendations were not predicated on CRSI having a financial interest in the acceptance or implementation of their recommendations.

[13] *See* workpaper entitled "Facility Security Assessment Executive Summaries."

recommendations from the FSA and the three additional factors discussed above: (1) the impact of the facility on electrical system reliability, (2) the number of employees at a facility and the number of visitors to the facility, and (3) the local crime rate. For example, although the number of employees at a particular facility may be relatively low, the critical nature of the facility for electrical system reliability and operations may call for increasing the security guard presence at that facility. In some cases, significant local crime rates likewise may suggest that a higher degree of security is prudent. In other cases, the remote location of a facility can delay response times by up to several hours, creating potential impacts that must be addressed. All of these factors were considered in forming SCE's enhanced security strategy.

c) Implementation of Enhanced Security Measures

It is important to enhance security at facilities that are critical to the reliability of the electrical grid and to better protect our employees and visitors. We are adding security guards at 22 facilities that do not currently have guards. We are also enhancing the qualifications for existing guards and adding armed officers at 22 other locations. This new approach to security will be phased in during 2013 and fully implemented by 2015, resulting in annual incremental O&M expenses of $15.240 million in 2015.

Also being phased in during 2013 and fully implemented by 2014 is the installation of metal detectors and X-ray scanners at nine key SCE locations, which will be staffed by armed guards.[14] This will result in increased annual O&M expenses of $10.250 million and $8.347 million for armed guards to staff the metal detection stations and the X-ray scanning equipment, respectively. Maintenance of the equipment will require an additional $2.5 million in annual O&M costs, including necessary equipment calibrations and reviews of monitoring procedures. These maintenance costs represent 5 percent of the overall capital costs outlined in Chapter II, Section F.2, which is SCE's standard rate for maintenance until capital costs are refined at an 80 percent confidence level.

d) Threat Management Program

Based on the best practices recommended by the American Society for Industrial Security (ASIS) and the Society for Human Resource Management (SHRM), in 2013, SCE formed a

[14] *See* the confidential workpaper entitled "SCE Security Enhancement, Controlled Access Areas, Metal Detection – Gensler." The workpaper is confidential because it contains specific details regarding the placement of security equipment at specific facilities.

Threat Management Team (TMT).[15] The TMT is responsible for assessing threats of workplace violence, developing risk-mitigation strategies, and formulating action plans in responding to potential threats of violence. Focusing on a prevention, detection, and mitigation strategy, the Corporate Security-led team is composed of management from cross-functional areas of SCE who work together to oversee the management and implementation of SCE's Workplace Violence Prevention Program (WVPP).

As part of the new threat management program, SCE engaged the services of a threat assessment consultant in 2013, Threat Assessment Group (TAG), to assist the TMT in providing training and threat assessment expertise. TAG is an internationally recognized threat assessment consultant with a strong background in psychiatry and psychology. TAG's participation as a member of the TMT provides the external forensic assessment recommended as part of the ASIS/SHRM best practices model. The annual cost for TAG's services is estimated to be $100,000 in O&M costs, consisting of an annual retainer of $25,000 and $75,000 a year for consulting services.

2. Edison Security Operations Center Staffing

Corporate Security is currently building a new Edison Security Operations Center (ESOC) to replace the existing and outdated Central Alarm Station (CAS). The ESOC will provide additional capacity to monitor, assess, and identify appropriate responses to alarms and intrusions while also providing sufficient physical space and systems connectivity for anticipated growth. Details regarding the capital expenditures for the ESOC project are detailed below in Chapter II, Section F.3.

With the migration of the central monitoring and response coordination functions to the ESOC, SCE will move existing CAS monitoring personnel to the ESOC. However, internal SCE supervisors will replace the current CAS contract supervisors, which will result in greater control and accountability and limit access to confidential information and security countermeasures to SCE employees. Staffing the CAS currently costs $1.04 million per year. Contract staff consists of 22 supplemental workers in a variety of roles, including operators, NERC-trained operators, leads, and supervisors. With the implementation of the ESOC, the staff will be comprised of five SCE supervisors and 17 contract control room operators, each of whom have been cross-trained in all functions of the

[15] *See* ASIS International, *ASIS Workplace Violence Prevention Program*, September 2011 (ASIS/SHRM WVPI.1-2011). This copyrighted publication is not included as a workpaper as ASIS International prohibits the reproduction and dissemination of the document.

ESOC monitoring stations. This staffing plan will provide four control room operators for the ESOC on a 24/7/365 basis.

Table II-2 below summarizes the future annual O&M costs for the 17 control room operators (2,080 hours per year, per operator, per shift) and five SCE supervisors (each with a market reference point salary of $87,300 per year). This results in an O&M cost of $1.258 million, an incremental increase of $215,000 per year from the current cost to operate the CAS.

Table II-2
Incremental O&M Increase for ESOC Staffing

Line #	Position/Total	Annual Cost ($000s)
1	Day Shift (6 operators @ $22.93/hr.)	286
2	Swing Shift (6 operators @ $23.26/hr.)	290
3	Grave Shift (5 operators @ $23.59/hr.)	245
4	SCE Supervisor (5 @ $87,300 annually)	437
5	Total future costs to operate ESOC (Line 1 + Line 2 + Line 3 + Line 4)	1,258
6	Current costs to operate CAS	1,043
7	Total incremental cost to operate ESOC (Line 5 - Line 6)	215

3. Security System Maintenance and Repairs

A recurring theme in the FSA recommendations was the need to improve security system maintenance. This includes the repair and maintenance of security systems at substations, power generating facilities, and non-electric facilities, such as service centers, payment offices, general offices, and data centers. Corporate Security requires additional funds to implement this recommendation and properly maintain existing security systems, improve badging, and maintain the additional security equipment being installed during the 2013-2017 period.[16]

Maintenance and repair deficiencies resulted from the need for Corporate Security to prioritize security installation support for NERC CIP physical security perimeters during 2008-2011. The deferral of maintenance and repair has resulted in many existing security system components passing their useful lives or being degraded due to wear and tear from multiple uses, weather conditions, facility power fluctuations, and other failure-mode producing factors. Repair and maintenance of the alarm system is necessary for key protection systems to operate as designed, allow security officers to

[16] *See* Chapter II, Section F.5., below for a discussion of the additional security equipment that will be installed.

respond to alarms when they occur, provide continued monitoring and protection of critical assets, and provide security officers with the tools needed to comply with regulatory mandates and protect SCE assets and personnel as well as visitors to SCE facilities.

The need to improve maintenance is highlighted by the many facilities with security equipment that is no longer manufactured, as shown in Table II-3 below.

Table II-3
Existing Security Equipment No Longer Manufactured

Manufacturer	Model Number	Description	Category
HID	Model 6445C	Magnetic Stripe Reader	Discontinued
HID	Model 230	Proximity Reader	Discontinued
Bosch	ZX-55	Analog Camera	Discontinued
Pelco	Spectra-III PTZ	Analog Camera	Discontinued
Pelco	IS-90	Analog Camera	Discontinued
Extreme CCTV (Bosch)	EX-46	Analog Dome Camera	Out of Business
Extreme CCTV (Bosch)	UF-500	Spot Illuminator	Out of Business
Gunnebo Omega	Optistile 100	Turnstile	Discontinued
Intrepid	RM-6	Perimeter Intrusion System	Discontinued
NICE Systems	Alto DVR	Digital Video Recorder	Discontinued
Samsung	SPD-2335N	Analog Camera	Discontinued
Samsung	SPD-2700N	PTZ Camera	Discontinued
Sanyo	VCC-4594	Analog Box Camera	Discontinued

Maintenance or repairs for equipment no longer manufactured may not be possible if replacement parts are not available or not supported by the manufacturer. As a result, equipment may stay in a deferred maintenance or repair state until the equipment is replaced or updated.

To properly maintain new security systems, address the degradation of existing systems, ensure adequate employee badge stock, and license security software and related systems equipment, Corporate Security requires an increase in non-labor O&M expense of $450,000 in 2015, which represents the difference between the $1.45 million total forecast for 2015 and the $1 million five year average of historical costs from 2008 to 2012. The funds will be used to maintain access control turnstiles, electronic identity badge readers, surveillance cameras, request to exit devices, electronic locks, intrusion detection equipment (door contacts), fence detection wiring, alarm panels, video recording systems, and visitor management readers. This cost estimate is based on recorded expenditures for existing facilities.

4. NERC CIP Security System Maintenance and Manual Observations

NERC CIP Standards require that all CCAs be contained within a defined physical security perimeter (PSP). A PSP is the six-wall physical border that surrounds an electronic security perimeter that contains a CCA. The PSP provides the first line of defense against cyber-attacks on cyber assets. Depending on the number of cyber assets within an electronic security perimeter, a PSP can range in size from a small cabinet to an entire building, and may have a number of access points.

NERC CIP-006 Standard, which sets the requirements for the physical security of BES cyber systems, requires SCE to restrict access to PSP access points, continuously monitor all access points for authorized and unauthorized access, and log and review all access. The 24/7/365 continuous monitoring, logging, and alarm reporting for PSPs is normally conducted by Corporate Security's security systems, which is referred to as the Physical Access Control System (PACS) in the NERC Standards. The PACS is a cyber-based system that supports the protection, access control, and monitoring of a PSP. As with all cyber systems, the PACS must be properly maintained and repaired.

NERC CIP Standards require immediate detection of, and responses to, any unauthorized access attempts and also require monthly assessment and installation of software patches to the PACS, which often requires taking the PACS offline for a planned period. As with any electrical or mechanical system, the PACS may require unscheduled maintenance, which can result in unscheduled monitoring outages. NERC CIP Standards require that SCE maintain compliance for physical protections and monitoring of physical security perimeters, even when the PACS environment is non-operational (*e.g.*, for maintenance or repair). As part of the NERC compliance program, during planned and unplanned monitoring outages (*e.g.*, scheduled software patch installation, unscheduled PACS outages, and firmware upgrade of the alarm panels), Corporate Security deploys on-demand security guards to observe and document all monitoring of access points. This is performed at each of the existing 35 NERC CIP physical security perimeters. Under NERC CIP v5, the number of NERC-regulated PSPs requiring monitoring is projected to increase to more than 140.

The increase in the number of sites impacted by NERC CIP v5 will increase the number of NERC regulated PSPs and the associated number of access points. This directly impacts NERC CIP security system maintenance and repair costs and the need for increased on-demand guard services. Corporate Security plans a minimum of six to eight outages per year to maintain the PACS system as required by NERC CIP-007, cyber security requirements, and other necessary maintenance or enhancements. To deploy on-demand security guards and perform the required system maintenance and

repairs at the additional facilities that will fall under the scope of NERC CIP v5, Corporate Security will require an O&M increase of $350,000 in 2015.[17]

D. Corporate Security Forecast (Portions of FERC Accounts 920/921)

1. Analysis of Recorded Costs

Corporate Security records labor and non-labor expenses to FERC Accounts 920/921. Corporate Security's portion of recorded O&M costs for Accounts 920/921 during 2008-2012 is set forth in Table II-4 below.

Table II-4
Corporate Security
Portions of FERC Accounts 920-921
2008-2012 Recorded O&M Expenses
(Constant 2012 $000s)

FERC Account 920-921	2008	2009	2010	2011	2012
Labor	3,039	3,415	3,862	4,500	4,781
Non-labor	7,538	7,449	8,533	9,429	9,865
Other	0	0	0	0	0
Total	10,577	10,864	12,395	13,929	14,646

From 2008 to 2009, total costs recorded to this account remained relatively stable. In 2010, total costs increased by 14 percent. This variance was driven by approximately $827,000 in non-labor costs for increased contract security guard services, an additional $500,000 in labor expenses for a new Physical Security Systems and Controls manager and new Technical Specialists, and $200,000 in non-labor costs for security technology maintenance expenses. From 2010 to 2011, total costs increased by 12 percent, or $1.753 million. This was driven by $663,000 in new contract security guard services required for NERC CIP compliance, $505,000 in overall contract security guard services for new SCE sites, and $585,000 in labor to staff the Corporate Security NERC CIP compliance effort. From 2011 to 2012, costs remained relatively stable.

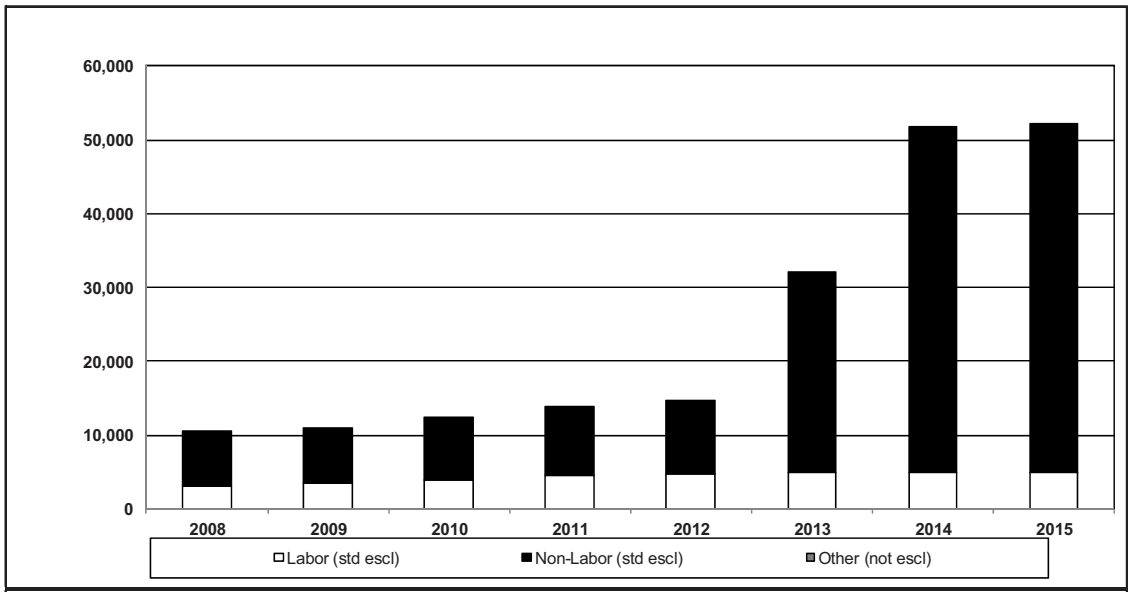
2. Test Year Forecast

The 2015 O&M forecast for Corporate Security's portion of FERC Accounts 920/921 is $52.098 million. This forecast is based on 2012 recorded expenses plus adjustments for the new

[17] *See* workpaper entitled "O&M Expenses for NERC CIP Security System Maintenance and Manual Observations."

programs and costs discussed above. The 2013-2015 forecast along with 2008-2012 recorded expenses is provided in Figure II-2 below.

Figure II-2
Corporate Security
Portions of FERC Accounts 920/921
2008-2015 Adjusted/Recorded and Forecast Expenses
(Constant 2012 000s)



	2008	2009	2010	2011	2012	2013	2014	2015
Labor	3,039	3,415	3,862	4,500	4,781	4,996	4,996	4,996
Non-Labor	7,538	7,449	8,533	9,429	9,865	27,033	46,692	47,102
Other	0	0	0	0	0	0	0	0
Total	**10,577**	**10,864**	**12,395**	**13,929**	**14,646**	**32,029**	**51,688**	**52,098**

Forecast

a) 2015 Test Year Base Forecast

Corporate Security's base 2015 forecast for ongoing activities is $14.646 million, which is the 2012 recorded expenses for both labor and non-labor expenses. Although labor and non-labor expenses have been steadily increasing through the 2008-2012 period, due in part to the increased scope of work and new NERC CIP compliance requirements, costs for the scope of work conducted during the 2012 base year are not expected to continue increasing in this manner. The increased O&M expense associated with the additional programs and scope of work discussed in Chapter II, Section C, is captured in future year adjustments to the last recorded year base forecast.

b) Future Year Adjustments to Base Forecast

To the 2015 Test Year base forecast discussed above, Corporate Security forecasts future year adjustments as shown in Table II-5 below.

Table II-5
Corporate Security
Portions of FERC Accounts 920/921
Future Year Adjustments and 2015 Test Year O&M Forecast
(Constant 2012 $000s)

Line #	Adjustment/Forecast	2013	2014	2015
1	Workplace Security and Grid Protection Improvements	17,018	36,437	36,437
2	ESOC Staffing	215	215	215
3	Non-NERC Security Systems Maintenance and Repairs	0	90	450
4	NERC CIP Security Systems Maintenance and Manual Observations	150	300	350
5	Total adjustments (Line 1 + Line 2 + Line 3 + Line 4)	17,383	37,042	37,452
6	2015 Test Year Base Forecast (see Chapter II, Section E.1.a)	14,646	14,646	14,646
7	2015 Test Year Total Forecast (Line 5 + Line 6)	32,029	51,688	52,098

Table II-5 above reflects the phasing-in of the Workplace Security and Grid Protection Improvements, non-NERC Security Systems Maintenance and Repairs, and NERC Security Systems Maintenance and Manual Observations during 2013 and 2014. The adjustments identified above for 2015 reflect full implementation of the programs described in Chapter II, Section C, above.

E. Background Investigations Forecast (FERC Account 923)

1. Analysis of Recorded Costs

Corporate Security records non-labor expenses in FERC Account 923 for a third party vendor to perform background investigations of candidates for new full time or contingent (contract status) employment. This account also includes non-labor expenses to conduct Personnel Risk Assessments (PRAs) required by NERC CIP-004 of any employee or contingent worker with direct or virtual access to CCAs. Table II-6 below shows the 2008-2012 recorded O&M expense for this account.

Table II-6
Background Investigations
FERC Account 923
2008-2012 Recorded O&M Expenses
(Constant 2012 $000s)

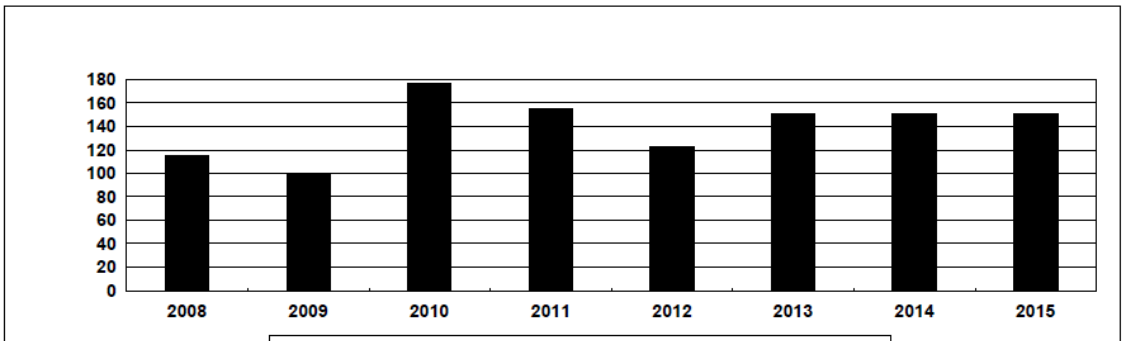
FERC Account 923	2008	2009	2010	2011	2012
Labor	0	0	0	0	0
Non-labor	115	99	177	155	123
Other	0	0	0	0	0
Total	115	99	177	155	123

Costs in this account fluctuated significantly throughout the 2008-2012 period. However, on an absolute basis, these fluctuations have been relatively small, peaking at $78,000 when expenses increased from $99,000 to $177,000 between 2009 and 2010. In general, the variability in this account is driven by changes in the number of background checks and PRAs performed each year. In some cases, the timing of invoicing by the outside vendor for these services may also play a role in year-to-year variations.

2. Test Year Forecast

Corporate Security forecasts 2015 Test Year expenses of $151,000 to conduct background investigations. The 2013-2015 forecast for this account, along with 2008-2012 recorded expenses, is provided in Figure II-3 below.

Figure II-3
Background Investigations
FERC Account 923
2008-2015 Adjusted/Recorded and Forecast Expenses
(Constant 2012 $000s)



	2008	2009	2010	2011	2012	2013	2014	2015
Labor	0	0	0	0	0	0	0	0
Non-Labor	115	99	177	155	123	151	151	151
Other	0	0	0	0	0	0	0	0
Total	**115**	**99**	**177**	**155**	**123**	**151**	**151**	**151**

Forecast

This forecast is based on a three-year average of 2010-2012 non-labor expenses. The averaging method is appropriate for this account as expenses have shown significant year-to-year fluctuations. This approach is consistent with D.89-12-057, in which the CPUC stated that for those accounts that have significant fluctuations in recorded expenses from year-to-year, an average of recorded expenses is appropriate to use as a basis for forecasting.

Historically, these fluctuations have been driven by costs for an outside vendor to perform background checks for contingent workers as well as PRAs for employees requiring access to critical cyber assets. On average, 191 PRAs were performed each year between 2010 and 2012. We expect this trend to continue through 2014. In 2015, NERC CIP v5 will significantly increase the number of CCAs, resulting in a corresponding increase in the number of PRAs conducted each year. Personnel who are assigned and/or need access to CCAs will require valid PRAs to be in place at the time access is granted. Additionally, existing employees who underwent PRAs in 2008 and 2009 will require new PRAs as PRAs must be renewed every seven years.

F. Corporate Security Capital

Corporate Security is requesting an increase of capital expenditures to improve workplace security, improve protection of business assets, and deploy security systems needed to comply with NERC CIP v5 Standards. The capital expenditures forecast for 2013-2017 is $137.881 million, as detailed in Table II-7 below.

Table II-7
Corporate Security Capital Expenditure Forecast Summary
(Nominal $000s)

Project Title	WBS ID	2012 (Prior Spend)	Forecast					
			2013	2014	2015	2016	2017	Total 2013-2017
Workplace Security Improvements	COS-00-CS-CS-741900	-	1,200	38,113	-	-	-	39,313
NERC/CIP Physical Security	COS-00-CS-CS-705100	-	10,420	10,000	14,881	-	-	35,301
Edison Security Operations Center	COS-00-CS-CS-SOCUPG	-	2,471	1,451	630	-	-	4,552
	COS-00-RE-BR-700700	190	1,988	-	-	-	-	1,988
	CIT-00-SD-PM-000138	1,386	6,576	1,113				7,689
New Physical Security Protection Systems (Blanket)	COS-00-CS-CS-SS	-	2,000	4,098	4,191	4,281	4,366	18,936
Security System Enhancement/ Refresh (Blanket)	COS-00-CS-SA-SAEP01	-	0	4,501	4,600	4,701	4,804	18,606
A-Substation Security Perimeter Improvements	COS-00-CS-CS-ASUBS	-	2,200	2,249	2,300	2,350	2,397	11,496
Total		1,576	26,855	61,525	26,602	11,332	11,567	137,881

The key drivers for Corporate Security's capital forecast are discussed in the following section. These drivers are consistent with challenges identified by a consortium of utilities and experts, as documented by the ASIS Utilities Securities Council with support from the Physical Security Council.[18] These factors drive SCE's need to add and/or improve physical protections of personnel and assets to reduce the probability and consequence of company damage/loss and emerging threats, all of which ultimately can impact SCE's ability to deliver safe and reliable electricity to SCE's customers.

[18] *See* ASIS International, *Utility and Smart Grid Security: The Impact of the NERC CIP Standards and NISTIR 7628 to the Utility Industry*, 2011. This copyrighted publication is not included as a workpaper as ASIS International prohibits the reproduction and dissemination of the document.

1. Key Drivers for Capital Expenditures

There are four key drivers for SCE's capital expenditure forecast: (1) improving workplace security and protecting grid reliability; (2) NERC CIP v5 compliance; (3) inconsistent and non-standardized security measures; and (4) aging security systems.

a) Improving Workplace Security and Protecting Grid Reliability

SCE is committed to protecting the electrical infrastructure critical to the reliable delivery of power while providing a safe work environment for our employees and visitors to our facilities. As discussed above in Chapter II, Section C.1, SCE has evaluated and reassessed its strategy for workplace security and protective services and has identified heightened security measures to improve workplace safety and the protection of grid reliability.

As part of this effort, SCE has identified a significant number of facilities that have no standardized security systems and/or, in some cases, on-site security officers. SCE intends to address this gap by adding new physical security systems and adding or enhancing on-site security officers. SCE also will be implementing controls to support a weapons prevention program at key facilities. Security at these facilities will also be enhanced by improving access controls, deploying new security systems, and refreshing and updating existing systems.

As part of the weapons prevention program, SCE is implementing a screening program consisting of metal detectors and X-ray scanning equipment installed at access points at nine key facilities. The screening program is designed to improve the detection of unauthorized weapons and materials to support overall workplace security and grid reliability improvements. Consistent with SCE's overall security strategy discussed in Chapter II, Section C.1, three primary criteria were used to determine at which facilities this equipment would be installed: (1) impact to business operations, (2) workplace population and visitor traffic, and (3) local crime statistics. An additional key component of the X-ray screening program is the integration of the X-ray equipment with the current alarm and response system to minimize response time in the event of a workplace violence incident.

b) NERC CIP Compliance

NERC CIP Standards provide a framework for protecting BES assets, along with specific compliance requirements. NERC CIP Standard 002-009 applies to control centers, communications essential to the energy control center, generation, and transmission and distribution electric facilities of 100kV and above. This is the core Standard that defines which critical cyber assets require protection. Critical cyber assets (CCAs) are programmable electronic devices, including the

hardware, software, and data in those devices, that are essential to the reliable operation of the grid. These critical assets are the facilities, systems, and equipment that, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES. Compliance with NERC CIP Standards is necessary to provide adequate protection of the cyber assets and minimize the potential for physical damage to critical equipment, significant service outages, impact to public safety, and unauthorized disclosure of confidential information.

Corporate Security is responsible for deploying and maintaining physical security controls for NERC CIP assets. The security controls include access controls, detection of unauthorized individuals, 24/7/365 monitoring and response, and a 15-minute response time for security incidents. SCE has gained valuable experience through the implementation of these control measures at facilities in connection with NERC CIP v3 Standards. SCE will now apply the security control standards implemented at these facilities to the expanded set of facilities that will be brought within the scope of NERC CIP regulations with the adoption of the NERC CIP v5 Standards.

c) Inconsistent and Non-Standardized Security Measures

During recent years, the prioritization of security system installation efforts for NERC CIP compliance, new substation security installations, and on-going changes in facility usage and employee populations has delayed Corporate Security from deploying security systems at facilities without a security system, or with minimal security system components. As described in Chapter II, Section C.1, in 2012, SCE conducted FSAs with an outside vendor, CRSI, to evaluate SCE's workplace security measures. CRSI identified several key issues impacting physical security at SCE, including the lack of security systems at some facilities, the lack of standardized security system monitoring, and the lack of key enterprise security practices, such as visitor management, access control to SCE facilities, and key policies for workplace security and workplace violence prevention.

The issues identified by CRSI and the FSAs drive the need to increase the deployment of security system installations at facilities without a security system and to expand security and access control systems in an integrated monitoring system. Deploying the security systems along with the enhanced security measures described in Chapter II, Sections C.1 and F.2, will provide needed improvements to the protection of assets, grid reliability, and personnel.

d) Aging Infrastructure

SCE has an ongoing refresh program for security system maintenance and updates for the continued operation of existing security systems and their integration with the enterprise security

monitoring system. Currently, many facilities have security systems that are beyond their service lives or operate at degraded performance levels.[19] The focus on new security system installations has created a backlog in security system refresh, which continues to grow based on the age and installation dates of the equipment. The refresh program has been unable to keep pace with the rate at which security systems become degraded or non-operational. During the FSA process, the external consultant confirmed that the refresh rate and maintenance of security systems at SCE are inadequate. To improve the refresh rate, Corporate Security has developed standards for repairs and replacement that will allow third party support to correct deficiencies in access controls, security surveillance, and asset protection.

To address these issues, SCE plans to increase spending on the existing security system refresh program. This effort includes the replacement of obsolete systems that are non-operational (*e.g.*, tape-style video recording devices, magnetic stripe readers), a refresh of existing systems that are operating at a degraded performance level (*e.g.*, partially operating intrusion detection systems, video surveillance equipment with poor image quality), enhancement of existing systems that do not comply with current physical security requirements for emergent threats (*e.g.*, converting local analog video to IP-based routable video surveillance for integration into the new ESOC), and replacement of equipment that has aged past its recommended service life (*e.g.*, certain perimeter intrusion detection systems are beyond their 15-year service life).

2. Workplace Security and Grid Protection Improvements

a) Background

The workplace security and grid protection improvements project is comprised of two distinct efforts discussed in Chapter II, Section C.1. The first is the implementation of a screening program to prevent unauthorized weapons and materials from entering the workplace. These new security measures are needed to enforce SCE's weapons prohibition policies by detecting weapons at facility access points and preventing them from entering SCE's facilities. The program includes the installation of metal detectors and baggage and parcel X-ray scanning equipment at key facilities, such as large office buildings, grid control and data centers, engineering headquarters, and call centers. In the second effort, SCE is adding security officers at 22 locations where no security officers are currently posted. These officers will require 2-way radios and kiosks.

---

[19] *See* Table II-3: Existing Security Equipment No Longer Manufactured, above.

(1) Project Overview

The new security measures for the screening program include access-control turnstiles, walk-through metal detectors, X-ray equipment to scan items individuals are carrying, and X-ray equipment to scan mail and parcels at mail and small cargo processing facilities. To operate the equipment and properly conduct access controls, SCE will also place specially trained contract security officers at the metal detection and scanning stations.

This project will redirect traffic flow for all ingress or egress on the identified campuses so that every person who seeks to enter will pass through metal detectors and subject their belongings to a scan for prohibited items. To achieve this level of control, SCE will install pedestrian turnstiles, walk-through metal detectors, and X-ray scanners at a limited number of entry points in each facility.

Metal detector and scanner installations require varying degrees of building modifications to accommodate the access control equipment, traffic flows, Americans with Disability Act considerations, and a multitude of local building, fire, and safety code requirements. In some cases, local code enforcement and plan approvals may trigger additional building modifications required by local officials.

Because of this complexity, the project plan will consist of preliminary security engineering drawings, specifications, bill of materials, and detail cost and schedule estimates. Corporate Security will require the services of an outside consultant and the SCE Corporate Facilities department to support the security engineering effort and cost estimations.

The second part of this project provides essential shelter and communications for the new security officers, which requires the purchase of 50 radios (900 MHz) and the build-out of security kiosks at the 22 locations where security guards will be added.

O&M labor and non-labor costs for this project are detailed in Chapter II, Section C.1. Table II-8 below provides the capital expenditure forecast for this project.

Table II-8
Workplace Security and Grid Protection Improvements
Capital Expenditure Forecast
(Nominal $000s)

	Forecast					
WBS ID	2013	2014	2015	2016	2017	Total
COS-00-CS-CS-741900	1,200	38,113	-	-	-	39,313

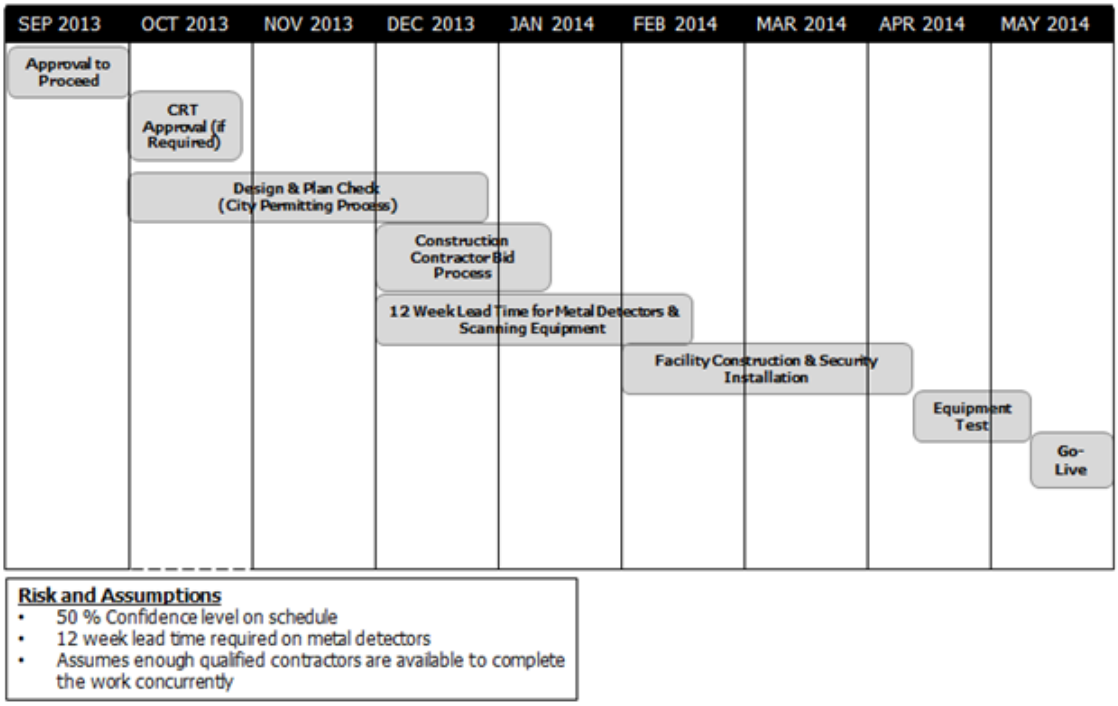
(2) Scope

The scope of the workplace security and grid protection improvements project is the installation of screening devices at nine locations having multiple buildings and facilities. Included are metal detectors, X-ray equipment for personal belongings and parcels, access control turnstiles, access card readers, emergency exit only (EEO) door controls, and associated modifications. Security officers will operate the equipment, pace the screening, evaluate the screening results, and conduct follow-up (secondary screening) as needed. The project also includes the purchase and installation of X-ray package and small cargo scanners for the locations where mail handling rooms are present, as well as capital expenditures required for the 50 radios and security kiosks for the security officer deployments at the 22 locations discussed above.

(3) Implementation Schedule

SCE will begin implementation during 2013 with the project completing in 2014. Figure II-4 below provides the current proposed/estimated implementation schedule for the installation of the metal detectors and X-ray scanning equipment.

Figure II-4
Workplace Security and Grid Protection Improvements
Proposed/Estimated Schedule



b) Business Drivers

It is important to take reasonable steps to deter, prevent, and mitigate threats by enhancing the level of security to support the reliability of SCE's electric system, and to better protect our employees and authorized visitors at business critical locations. Several recent serious incidents demand a robust response and preventative action plan by SCE, including: (1) the April 15, 2013 Boston Marathon bombing incident, which is being investigated by the police and FBI as a terrorist incident and potential bell weather for individually driven terrorist attacks in the United States, (2) the April 16, 2013 PG&E Metcalf Substation transformer shooting and fiber-optic cable cuts, which is also being investigated by local police and the FBI, and (3) the December 16, 2011 Rivergrade workplace shooting incident.[20]

[20] *See* workpapers entitled "CNN: Boston Marathon Terror Attack Fast Facts," "CBS: Vandalism at San Jose PG&E Substation Called Sabotage," and "SCE Press Release: Fatal Shootings at Southern California Edison Irwindale Facility."

c) Forecast Expenditures

Facility and Corporate Security expenses for the installation of the metal detectors are estimated at $25 million, as shown in Table II-9 below.[21] Installation costs include architectural and engineering designs, equipment costs, SCE costs, and a 15 percent contingency.

Table II-9
Metal Detector Facility and
Corporate Security Costs

Location	Facility Costs ($)	Corporate Security Cost ($)	Total Cost ($)
Alhambra Data Center	427,912	208,708	636,620
Alhambra Grid Control Center	1,716,034	323,294	2,039,328
Edison Education Center	993,498	225,599	1,219,097
General Office 1 (1st Floor)	2,060,906	340,744	2,401,650
General Office 1 (Garage)	1,822,993	447,586	2,270,579
General Office 2	1,038,590	48,671	1,087,261
General Office 3	1,063,243	311,997	1,375,240
General Office 4	688,172	309,923	998,095
General Office 5	1,157,287	721,768	1,879,055
Irvine Operations Center	560,583	230,564	791,147
Irwindale Business Center	1,414,323	698,892	2,113,215
Long Beach Regional Office (1st Flo	1,884,655	535,350	2,420,005
Pomona Innovation Village - Building	556,414	627,354	1,183,768
Pomona Innovation Village - Building	557,506	626,468	1,183,974
Rancho Cucamonga Regional Office	1,049,786	591,705	1,641,491
Rivergrade Complex Building 3	964,236	794,908	1,759,144
Total	17,956,138	7,043,531	24,999,669

The purchase and installation of the X-ray scanning equipment will result in an additional $13.344 million in capital costs as shown in Table II-10 below.

[21] *See* confidential workpaper entitled "SCE Security Enhancement, Controlled Access Areas, Metal Detection – Gensler."

Table II-10
X-ray Scanning Equipment
Purchase and Installation Costs

Location	# of Baggage Scanners	Baggage Scanner Cost (@ $23,759 each)	# of Parcel/ Mail Scanners	Parcel/Mail Scanner Cost (@ $44,337 each)	Total Scanners (Baggage + Parcel/Mail)	Scanner Installation (@ $289,536/ scanner)	Total
Alhambra Data Center	1	23,759	1	44,337	2	579,072	647,168
Alhambra Grid Control Center	1	23,759	0	0	1	289,536	313,295
Edison Education Center	1	23,759	0	0	1	289,536	313,295
General Office 1	2	47,519	0	0	2	579,072	626,591
General Office 1 (Garage)	1	23,759	1	44,337	2	579,072	647,168
General Office 2	1	23,759	0	0	1	289,536	313,295
General Office 3	1	23,759	0	0	1	289,536	313,295
General Office 4	2	47,519	0	0	2	579,072	626,591
General Office 5	4	95,038	1	44,337	5	1,447,680	1,587,055
Irvine Operations Center	1	23,759	1	44,337	2	579,072	647,168
Irwindale Business Center	1	23,759	1	44,337	2	579,072	647,168
Long Beach Regional Office (1st Floor)	3	71,278	1	44,337	4	1,158,144	1,273,759
Pomona Innovation Village - Building 1	3	71,278	1	44,337	4	1,158,144	1,273,759
Pomona Innovation Village - Building 3	3	71,278	0	0	3	868,608	939,886
Rancho Cucamonga Regional Office	4	95,038	1	44,337	5	1,447,680	1,587,055
Rivergrade Complex Building 3	4	95,038	1	44,337	5	1,447,680	1,587,055
Totals	33	784,062	9	399,033	42	12,160,512	13,343,607

The $970,000 in costs for the 50 radios and security kiosks to support the new security officers are detailed in Table II-11 below.

Table II-11
Costs for New Security Officer Support

Project Component	Units	Unit cost ($)	Total Cost ($)
Radios (900 MHz)	50	4,000	200,000
Security Kiosks	22	35,000	770,000
Total			970,000

d) Project Justification

The purpose of the workplace security improvements is to protect facilities that impact grid reliability (*e.g.*, grid control, switching centers, and data centers), our ability to communicate with customers (*e.g.*, call centers and the customer educational facility), SCE's engineering headquarters, and the safety and security of locations with the largest employee and visitor traffic (*e.g.*, SCE's corporate headquarters). As detailed in Chapter II, Section C.1, SCE conducted a detailed

analysis of our facilities using an outside consultant as well as in-house experts to evaluate our facilities and ascertain methods to improve security.

As discussed above, the identified list of locations at which enhanced security will be implemented was based on a combination of three basic factors: (1) the criticality of the facility to the integrity and reliability of the electrical system, (2) the number of employees located at those facilities and the number of visitors to the facilities, and (3) the local crime statistics for those locations. SCE then prepared a matrix of those selected facilities and potential enhancements to heighten security measures at our most critical facilities. The most immediate and effective measure is to implement metal detectors staffed by armed contract security officers at nine locations to screen all employees and visitors to these key facilities, and deploy security guards at 22 locations that currently have no security presence.

3. NERC/CIP Physical Security

a) Background

As explained by Mr. Pespisa in Exhibit SCE-09, a revised version of the NERC CIP Standards is expected to become effective in October 2015 and will substantially increase SCE's compliance requirements. The NERC CIP v5 Standards include a number of new requirements, but affects SCE most dramatically by requiring strictly defined physical and electronic protection measures to be applied to significantly more assets and systems than the version currently in effect (v3).

The NERC CIP v5 Standards create somewhat different terminology than the current and prior versions and identify cyber security requirements for protection of the BES cyber systems. The NERC CIP v5 Physical Security Standard (NERC CIP-006-5) defines the requirements for physical security of BES cyber systems. The purpose of the Standard is to define a security program to manage physical access and controls to BES cyber systems. It consists of three high level and 13 subpart requirements.[22] To comply with the Standard, a physical security plan must be used to document how SCE will meet each of these requirements. Compliance with the Standard is based on this physical security plan, which defines the processes, tools, and ratification that will be used to comply with the CIP-006 physical security requirements.

[22] The three high level requirements are: (1) R1 – Physical Security Plan for Protection of BES Cyber System, (2) R2 – Visitor Control Program, and (3) R3 – Physical Access Control System (PACS) Test and Maintenance.

As part of the overall NERC CIP Standards, each cyber system is categorized with an impact rating to the BES. CIP-006 defines a set of physical security protection measures, access controls, and monitoring requirements for each impact rating. The classification of cyber system impacts to the BES is defined in CIP-002 v5. CIP-006 v5 requires varying protection levels based on the four classification levels of a cyber system. Table II-12 below provides SCE's estimate for the total number of existing cyber systems, by classification level, that will require protection systems under NERC CIP v5.

Table II-12
NERC CIP v5
Deployment Schedule for Physical Security Perimeters

BES Rating	Projected Physical Security Perimeters
High Impact BES	17
Medium Impact BES with External Routable Connectivity (ERC)	17
Medium Impact BES without ERC	22
Low Impact BES	86+

(1) Project Overview

The physical security of BES cyber systems is the first line of protection against incidents that can impact BES operations. As reflected in Table II-12 above, the NERC CIP-006 v5 Standard will require SCE to deploy cyber security and physical security protections at more than 100 PSPs not covered by the current NERC CIP Standards. To comply with NERC CIP v5, SCE also will need to make modifications to the existing 35 PSPs that currently have physical security systems under the NERC CIP v3 Standards.

Corporate Security is responsible for managing and deploying the physical security controls for the BES cyber systems covered by the NERC CIP-006 v5 Standard. This requires Corporate Security to create a NERC CIP v5 compliant security program, which includes preparing formal security plans and the implementation of physical security perimeters (PSPs) around each BES Cyber Asset, BES Cyber System, or a Physical Access Control System (PACS) and Electronic Access Control System (EACS). The security program must also detail how SCE will address the access controls, logging, monitoring, and 15-minute response time requirements.

Corporate Security has deployed and managed the PSPs, and the related compliance efforts, for the facilities currently subject to the NERC CIP-006 v3 Standard. The changes

in requirements from v3 to v5 will require additional security controls and infrastructure at electric facilities within the broader scope of NERC CIP v5. SCE expects the Federal Energy Regulatory Commission (FERC) to issue an order that will require electric utilities, including SCE, to comply with the NERC CIP v5 Standard within a 24-month timeframe. Given the number of facilities impacted by NERC CIP v5, Corporate Security has developed a plan to modify the existing PSPs and deploy new PSPs within the anticipated 24-month compliance timeframe. Table II-13 below provides the cost forecast for this project.

Table II-13
NERC CIP Physical Security
WBS ID and Forecast Capital Expenditures
(Nominal $000s)

	Forecast					
WBS ID	2013	2014	2015	2016	2017	Total
COS-00-CS-CS-705100	10,420	10,000	14,881	-	-	35,301

(2) Scope

The scope of the NERC CIP Physical Security Program is to design and deploy PSPs at facilities subject to the NERC CIP v5 Standard. The perimeters are to be deployed as part of a physical security program to physically protect cyber systems that meet NERC CIP Standard criteria. The PSPs provide the first layer of defense and security to prevent unauthorized cyber access that could impact the operation of the BES, the delivery of electricity to SCE customers, and disaster recovery efforts.

The scope of the NERC CIP-006 v5 physical security program also includes the overall planning, design, deployment, commissioning, and continuous monitoring of each NERC CIP designated PSP, which is commensurate with the BES classification of High, Medium ERC, Medium or Low, as defined in NERC CIP v5 Standard. As part of the monitoring requirements under NERC CIP-006 v5, each of these PSPs will be integrated with the Edison Security Operations Center (ESOC, discussed in Chapter II, Sections C.2 and F.4), where monitoring and incident response for unauthorized physical access attempts will be assessed, responded to, and documented. The integration of the ESOC to the PSPs will allow Corporate Security to meet the NERC CIP requirements for continuous monitoring, 15-minute response times to physical security incidents, and access controls. The PSPs deployed under the NERC CIP v5 physical security plan will primarily use security system

equipment and telecommunications connectivity to provide real-time data to the ESOC. The alarm system will be designed to provide detection of authorized and unauthorized access, access logs, video surveillance of access points, and detection of forced intrusion.

Existing PSPs for cyber systems covered by the NERC CIP v3 Standard will be upgraded to meet the NERC CIP-006 v5 Standard. PSPs will be implemented at facilities that do not currently have them, based on the facility's BES impact rating. PSPs will be deployed at High impact-rated facilities first, followed by Medium with ERC, Medium without ERC, and then the Low impact facilities. This impact-based approach will further the goal of securing critical facilities that support the operation of the power grid.

Each PSP will be designed with a 6-wall border to protect its associated cyber system asset(s). As part of the perimeter security controls, all access points are controlled with factors of authentication (types) associated to access control (keys, card readers, special locks, etc.), intrusion detection devices for identification of unauthorized access, and to determine if entries and exits are authorized. Additional security equipment (such as cameras, alarm panels, relays, and other devices) is deployed to support monitoring of the PSPs, including remote monitoring by the ESOC.

Corporate Security will develop an integrated plan to perform the physical security designs, construction requirements, and installation of the security components. We will manage the installation and integration of the physical security systems with affected OUs, including Information Technology (IT), Regulatory Operations, and the Law department. We will also support the development of training for authorized personnel using the PACS and visitor management systems, including the development of incident response procedures for personnel in the Grid Operations, Substation Construction & Maintenance, Substation Test, and Substation Reliability functions.

(3) Implementation Schedule

The effective date for NERC CIP v5 Standard is expected to be October 1, 2015. To comply with NERC CIP v5 by this date, SCE will have to implement a tiered deployment to avoid impacts to key Transmission and Distribution (T&D) activities, including Grid Operations, Substation Construction & Maintenance, and Engineering. The PSPs will be deployed in advance so that required personnel can be trained and provisioned for access, and that their PRAs are completed before the effective date. SCE anticipates that as many as 3,000 personnel will require training, PRAs, and documented provisioned access before the effective date. Based on SCE's experience with the roll-

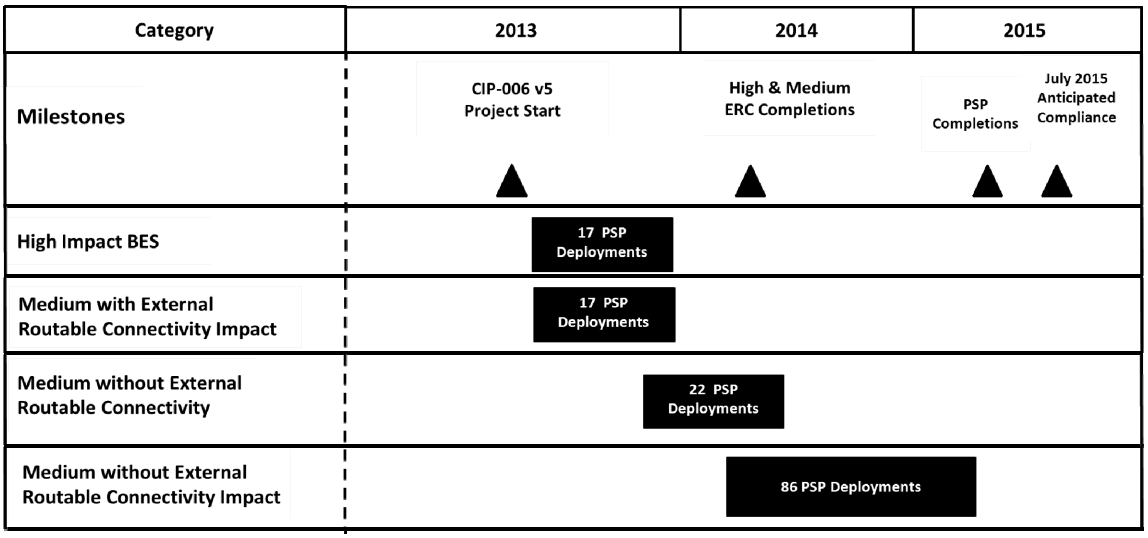
out of NERC CIP v3 PSPs, it is critical to resolve security system operation and personnel requirements well before the compliance deadline.

An additional challenge in the timely completion of the PSP installations is the availability of qualified security suppliers and vendors, which are finite in number. These security integrator resources, trained in security components used by SCE, are expected to be in high demand nationally, as all utilities will face the same NERC CIP v5 compliance deadline. As shortages in material and qualified vendors are expected, a tiered deployment solution is not only prudent, but necessary.

Each PSP system installation takes an average of three to four months. The installations require multiple steps: (1) creating engineering drawings, (2) developing the facility engineering requirements for power, infrastructure, and telecommunications, (3) planning out the construction with T&D and local city governments, and (4) performing the security installation, testing, and certification. Each facility presents engineering and construction challenges based on available space for the PSP and cyber asset, age of the infrastructure, and the availability of required resources (power and telecommunications) to allow for alarms to be integrated with and monitored by the ESOC. Once the security system is installed at a facility, all employees that will have access to the perimeter will be processed through an authorized list, and then undergo the required training. Only when all of this is achieved will SCE be able to demonstrate compliance.

The total number of PSPs, 142, is the primary driver mandating a timely start and tiered deployment of the PSPs as shown in Figure II-5 below.

Figure II-5
NERC CIP v5 Physical Security Perimeters
Deployment Schedule



b) Business Drivers

The business driver for deploying physical security of BES cyber systems is protecting against physical and cyber-attacks that could lead to misoperation of the grid and impact the delivery of electricity and disaster recovery efforts. To accomplish the installation of 107 new PSPs and modification of the existing 35 PSPs, we will design and deploy PSPs over time, based on the facility's BES impact rating. This prioritized approach of physical security deployments has been coordinated with T&D. The approach reduces the business impacts to T&D and security vendors, and establishes a compliance strategy that mitigates physical and cyber-attacks on facilities based on their importance to the BES. The time and effort required to design security systems, review with city planners, obtain competitive bids, install new or enhanced telecommunications infrastructure, and perform the security installations drive the need to spread the work over the 24 month period. In addition, T&D and Corporate Security will require adequate time for deployment, training, and integrating the effort into a compliance program prior to the anticipated compliance date.

c) Forecast

Table II-14 below provides a breakdown of the costs associated with this project.

Table II-14
Physical Security Perimeter Installations
Forecast Expenditure
(Nominal $000s)

Line #	Adjustment/Forecast	2013	2014	2015
1	Security System Hardware	6,296	5,996	8,994
2	Vendor Labor	3,101	2,953	4,430
3	SCE Labor	1,044	944	1,492
4	Total (Lines 1 + 2 + 3)	10,441	9,893	14,916

The expenditure for the physical security of BES is forecast based on the tiered approach discussed above and shown in Table II-14 above. A typical security and alarm system to secure a PSP costs approximately $249,000, excluding major issues or challenges to the infrastructure. PSPs are independent security protection layers for specific cyber assets that can affect the operation of the power grid. Each PSP is comprised of a physical access control system (alarm panels, power supplies, card readers and anti-tailgate devices at an approximate cost of $100,000) and video surveillance equipment (cameras and network video recorders at roughly $149,000). These PSPs will be integrated into the new ESOC, but are separately operating security systems with added protections to prevent tampering and electronic intrusions. Each year's cost forecast is based on the number of PSP installations forecast for the year, multiplied by the estimated average security system cost.

d) Project Justification

NERC CIP v5 Standards will require full compliance by the effective date. SCE's implementation plan described above will meet that requirement in an efficient and cost-effective manner by prioritizing based on the highest impact to the BES.

SCE's tiered approach will limit potential compliance risks. The complexity of installing new NERC CIP physical security perimeters will impact business operations in the IT and T&D OUs. Not using the tiered approached could increase compliance risks sites arising from issues relating to the accuracy of training, documentation, and deployment. Additionally, the tiered approach will avoid rushed field engineering and poorly executed installations of physical security systems, which could also increase non-compliance risks. A systematic, tiered approach to installing PSPs will permit the orderly and timely deployment of more than 140 compliant security systems and avoid compressed

timelines and delayed installations that can lead to early programmatic failures in terms of security system issues, personnel training issues, and documentation issues that could lead to non-compliance with NERC CIP Standards.

This project, in combination with the ESOC project discussed in Chapter II, Section F.4, provides the most cost-effective and lowest-risk solution for SCE to meet the NERC CIP Standards. As an alternative, SCE considered deploying security guards at every access point at the 142 PSPs to address access control, manual logging of personnel and visitors, and real-time response to threats. This approach would, in theory, satisfy the CIP-006 v5 Standards. However, the cost to support 24/7/365 guard staff would increase annual O&M expense by over $50 million, making this a non-viable option when compared to the less costly capital project option.[23] Additionally, this alternative option increased compliance risks as it relies on people – security guards, whose turnover rate is high – instead of a purpose-built, robust, electronic, automated access control systems. The capital expenditure is the most cost-effective way to establish, maintain, and demonstrate compliance with NERC CIP-006 v5 Standards.

The costs associated with the technology solution described above provide greater economic and grid reliability benefits to rate payers and SCE, in contrast to the projected ongoing O&M expenses necessary to meet NERC CIP Standards with the use of security guards. Expanding the capability and capacity of the PACS, installing the new ESOC, and replicating the PSP architecture at all affected facilities will effectively meet NERC CIP requirements and produce automated electronic access records, compliance artifacts, and repeatable automated real-time response to threats to SCE facilities, assets, and personnel.

4. Edison Security Operations Center (Including Information Technology and Operational Services Components)

a) Background

SCE will be transitioning its centralized alarm monitoring facility from the existing Central Alarm Station (CAS) to the Edison Security Operations Center (ESOC). The CAS was built in the 1980s for the original purpose of monitoring alarms and facilitating response for fire, safety, and emergency services at the SCE General Office complex in Rosemead, California. As SCE's footprint has grown over the past 25 years, the CAS has been pressed into service as the centralized

[23] *See* workpaper entitled "Cost Effectiveness of NERC CIP Compliance Projects."

alarm monitoring station for over 110 facilities within the SCE territory. With the introduction of the initial NERC CIP Standards in 2009, the CAS was designated as the primary facility for physical security monitoring of all NERC CIP cyber assets and controlled areas. Compliance with the NERC CIP alarm and monitoring requirements necessitated fitting additional staff and work stations into the small CAS space. The combination of increased staffing and a lack of major technology upgrades for the past 25 years has created an operational risk to SCE in monitoring physical security using the existing CAS.

Located in a 288 square foot room (18 feet x 16 feet) and using antiquated and obsolete security monitoring technology, the CAS can no longer be expanded to meet the increased alarm and access control monitoring demands that will come with the planned expansion of SCE's security system installations. The forecast growth in security monitoring necessary to protect company assets and personnel is driven by ongoing theft of material and equipment, vandalism/damage to SCE facilities and assets, and new security controls that are required by the upcoming NERC CIP v5 standard.

(1) Project Overview

The ESOC is a new centralized alarm monitoring facility that is designed to replace the existing CAS and support the expansion of physical security monitoring for new security system deployments as forecast by the workplace security improvements, substation security system installations, and the NERC CIP v5 compliance efforts. The ESOC will be integrated into an existing facility with backup power and telecommunications to support 24/7 operations. Security monitoring stations in the ESOC will provide real-time monitoring capability of access controls and alarm events at SCE business facilities, electrical facilities, and NERC-regulated cyber system assets.

The ESOC will utilize a physical security information management (PSIM) tool to improve incident and response management for all alarm events at SCE. The tool integrates the existing physical access control system, visitor management, video surveillance, and security call recording systems into a single interface, which will significantly improve the evaluation and response time for managing security incidents. This new capability will allow SCE to meet the NERC CIP-006 v5 Standard, which establishes a 15-minute timeframe for incident response of alarm or unauthorized access attempt to NERC CIP protected cyber assets. By transforming manual procedures to an automated work flow process using the PSIM tool will also reduce human error and judgment errors by eliminating the need to interpret written procedures. Video surveillance data, employee

records information, employee access information, intrusion alarms, and other security data is provided in synchronous (or continuous) sequence as part of each step in the work flow actions. This capability will allow increased consistency in responses to alarms and security incidents.

An enterprise visitor management tool will also be deployed as part of the ESOC effort. The enterprise visitor management tool is aimed at eliminating errors and inconsistent usage of the current manual visitor logging system across SCE. The lack of an enterprise visitor management system was identified as an enterprise security deficiency by CRSI during the FSA process. To avoid errors and correct these deficiencies, the ESOC project will integrate the enterprise visitor management system with the physical access control system's logging capability and create a single access control and visitor management log repository. The repository will be used to improve compliance with the NERC CIP-006 Standard and to identify visitor management deficiencies across SCE. Table II-15 below provides the cost forecast for this project.

Table II-15
Edison Security Operations Center
Capital Expenditures Forecast

	Capital Expenditures (nominal $000)						
WBS ID	2012 (Prior Spend)	2013	2014	2015	2016	2017	Total
COS-00-CS-CS-SOCUPG	-	2,471	1,451	630	-	-	4,552
COS-00-RE-BR-700700	190	1,988	-	-	-	-	2,178
CIT-00-SD-PM-000138	1,386	6,576	1,113	-			9,075

(2) Scope

The scope of the ESOC project covers the construction of a new centralized monitoring facility capable of supporting the growth in physical security monitoring for the next 15 years. As part of the scope, all current physical security monitoring for existing facilities and NERC CIP assets will be migrated to the ESOC. This effort includes integration of the PSIM tool with

SCE's physical access control system, video surveillance, intrusion detection, security call recording, and the enterprise visitor management systems.

The physical access control system will be integrated with the PSIM tool to improve consistency, quality, and accuracy in incident identification, tracking, and response. The tool will also standardize the response and escalation process to consistently meet the 15 minute response time required by NERC CIP-006 v5. The tool optimizes the use of all existing security applications so that all situational awareness data (video, alarm data, maps, and video analytics) is provided in real time to the responsible monitoring guard/stations. To support NERC CIP-006 compliance for incident response reporting, the PSIM tool will also be used as the central repository for incident and response data, incident report history, and compliance logs. This will reduce the evaluation of and look-up times for security-related incidents.

(3) Implementation Schedule

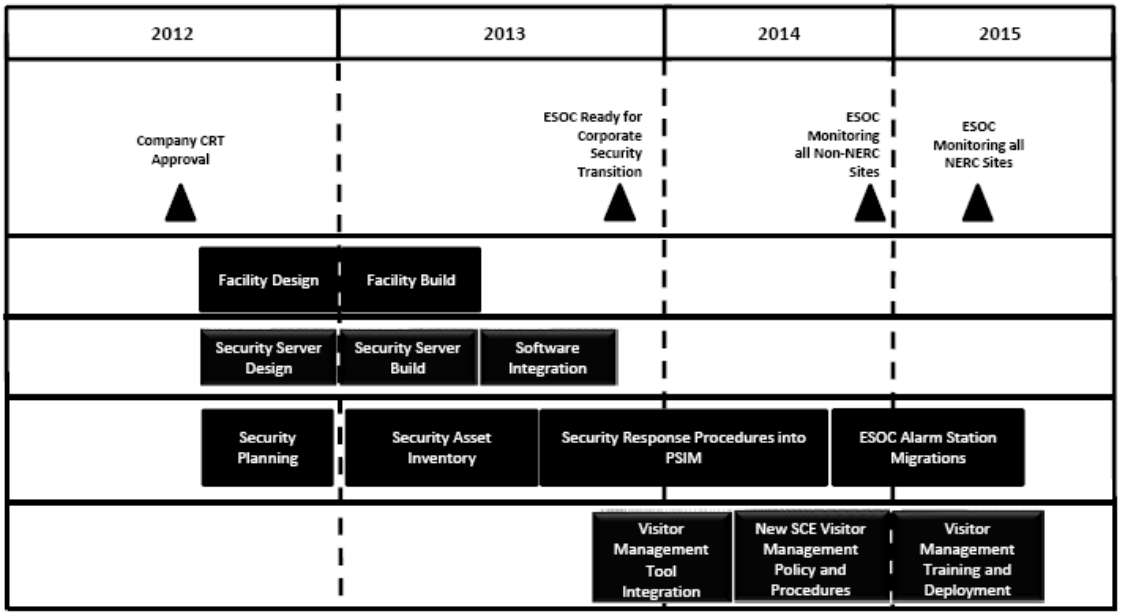
The ESOC project integrates many key functional activities within SCE, including Information Technology, Corporate Real Estate, Corporate Security, and Corporate Communications. An integrated project plan is used to identify key milestones, which are then used to plan out the project. Table II-16 below reflects key project milestones and scheduled completion dates.

Table II-16
ESOC Key Milestones and Completion Dates

Milestone	Scheduled Completion Date
Internal SCE Approval	7/31/2012
Complete ESOC Design	12/31/2012
Start Facility Construction	12/31/2012
Complete Security Server Installation	5/31/2013
Complete Facility Construction	8/31/2013
Complete Security Application Integration	12/31/2013
Complete ESOC Non-NERC Monitoring	9/31/2014
Complete ESOC NERC Monitoring	12/31/2014
Start Enterprise Visitor Management	2/28/2015
Complete Local Guard Station Migration	6/30/2015

Completion of the ESOC facility is scheduled for July 2015, as shown in Figure II-6 below.

Figure II-6
ESOC Implementation Schedule



b) Business Drivers

As detailed above, the existing CAS and its overloaded and obsolete systems create a substantial operational risk in SCE's ability to support the planned expansion of physical security monitoring, which is a key component of the security system installations. As discussed, these installations are driven by workplace security improvements, protection of critical electric facilities, and the security system enhancements needed to comply with NERC CIP v5 requirements. At approximately 2,000 square feet, the new ESOC eliminates scalability issues with increased staffing, work space, work stations, and additional monitoring of alarm facilities and access controls at SCE for the next 15 years. The ESOC will support compliance with the NERC CIP-006 Standard's 15 minute response time requirement and allow such responses to be handled in a repeatable, structured, and time-sensitive manner.

c) Forecast Expenditures

For the 2012-2015 period, $15.810 million is to be spent to construct and deploy the new facility and install the security software applications for the ESOC. Approximately $630,000

will be spent in 2015 to upgrade local and regional security guard station computers to allow security officers to utilize the new visitor management and PSIM software.

Table II-17 below shows the total capital forecast expenditures for the ESOC.

Table II-17
ESOC Forecast Expenditures
(Nominal $000s)

Line #	Expense Component	2012 (Prior Spend)	2013	2014	2015	2016	2017
1	Hardware	1,193	0	0	630	0	0
2	Software	0	2,791	0	0	0	0
3	CS Labor	105	822	1,392	591	0	0
4	CAS Materials	0	210	1,026	0	0	0
5	IT Labor	226	2,394	0	0	0	0
6	Facilities	190	1,988	0	0	0	0
7	Contingency	0	1,823	425	0	0	0
8	Total (sum of lines 1 through 7)	1,714	10,028	2,843	1,221	0	0

d) Project Justification

In addition to addressing the operational risks posed by the overloaded and obsolete monitoring capabilities of the existing CAS, the ESOC will work in concert with the NERC/CIP Physical Security project discussed in Chapter II, Section F.3., to meet the requirements of the NERC CIP Standards. The combination of these two projects provides the most cost-effective and lowest-risk solution to meeting the NERC CIP requirements.

As discussed above, the CAS is not capable of handling the substantial increase in security monitoring needed to support the new physical security controls required for compliance with the NERC CIP Standards. Without the ESOC, SCE would have to deploy security guards at every access point to each PSP to address access control and monitoring, manual logging of all access and attempted access, and real-time response to threats. As discussed, 24/7/365 guard staff support would increase O&M expense by over $50 million, making this a non-viable option when compared to the less costly capital project option.[24] Another alternative considered was to continue using the CAS and

[24] *See* workpaper entitled "Cost Effectiveness of NERC CIP Compliance Projects."

address its capacity limitations by distributing the security monitoring function among other locations. However, this non-centralized approach would result in increased complexity in communications and security logistics and increase compliance risks.

In addition, the more than 140 PSPs that will require monitoring under the NERC CIP v5 Standards will result in a substantial increase in access and visitor logging requirements. This will further strain the current manual documentation process and result in increased compliance efforts throughout SCE to confirm that we are properly managing and documenting all access logs and responding to security incidents in conformance with the strict NERC CIP Standards. The ESOC project, which supports the centralized and automated monitoring of access controls and real-time review of all access and visitor logs, provides a lower risk solution to deal with the significant expansion of PSPs.

Additional benefits the ESOC will provide include the improved monitoring of SCE assets, employees, and visitors, which will improve Corporate Security's ability to track and timely respond to security incidents. Newer security infrastructure and tools provide tighter controls for managing access to SCE facilities, as well as improve disaster recovery planning and security reporting. Postponing or eliminating this project would create a significant risk to NERC CIP-006 v5 compliance, which would require SCE to incur significant and recurring O&M costs to manually monitor the large number of security system perimeters until a technology solution is deployed.

5. New Physical Security Protection Systems (Blanket)

a) Background

The Physical Security Protection System program is an on-going effort to improve the physical protection of SCE assets and facilities that began in 1993 in response to rising incidents of thefts, break-ins, and other security incidents at SCE facilities. Continuation of this project was authorized in both the 2009 and the 2012 GRCs.[25] The overall purpose of adding physical security protection at SCE facilities is to reduce the number of security incidents that affect SCE operations, improve response to security incidents, and protect SCE personnel, assets, and the public. Providing a safe and secure workplace and protecting SCE assets greatly reduces the risk of catastrophic or severe

[25] D.09-03-025, pp. 244, 387; D.12-11-051, p. 587. *See* workpapers entitled "2009 GRC Decision Excerpts" and "2012 GRC Decision Excerpt."

impact to SCE's business operations, as well interruptions to electrical service caused by theft, vandalism, or damage at key SCE facilities.

Over its 20-year history, the objectives of the Physical Security Protection System program have been to: (1) deter theft and vandalism, (2) improve safety and access control for employees, customers, and visitors, (3) improve video surveillance of SCE assets and facilities, and (4) improve the protection of critical grid components. Over time, the program has focused on standardizing facility access controls, identifying personnel, improving the monitoring of alarms and key business assets, and responding effectively to incidents.

(1) Project Overview

The Physical Security Protection System program has historically included new security system installations as well as upgrades to existing systems as technology has evolved or systems reach the end of their serviceable life. Beginning in 2010, the scope of this project was limited to include only installations of new security systems where none existed before. Upgrades to existing security systems are now addressed by the Security System Enhancement/Refresh project discussed in Chapter II, Section F.6. Table II-18 below shows the recorded and forecast expenses for the project.

Table II-18
New Physical Security Protection Systems (Blanket)
2009-2012 Recorded and 2013-2017 Forecast Capital Expenditures
(Nominal $000s)

WBS ID	Recorded					Forecast					
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
COS-00-CS-CS-SS	2,472	2,331	119	982	602	2,000	4,098	4,191	4,281	4,366	18,936

Corporate Security plans to increase spending on new security and protection systems based on the high number of facilities that do not yet have standardized security systems. These efforts include the addition of visitor management kiosks, guard stations, video or closed circuit television (CCTV) surveillance, and access control based on the corporate identification badge. The present spend rate and security system deployment rate cannot achieve the necessary protection levels for workplace security and to mitigate loss by theft or vandalism, or damage to SCE infrastructure.

New security system installations have been identified as vital to safety and security at electric and non-electric facilities that have no existing physical security protection,

access control, and intrusion detection systems, or integrated alarm management and response coordination with the ESOC. The list of facilities requiring installation of security systems and security projects are prioritized and selected based on the facility's impact on business operations and the delivery of power to customers. These new installations address the gaps identified in the FSAs discussed in Chapter II, Section C.1, which highlighted the inconsistent deployment of security controls across SCE.

Ongoing incidents of vandalism, metal/copper theft, and resulting damage to SCE business facilities, such as substations and service and payments centers, have a significant effect on the operation of the grid, repair and maintenance activity at service centers, and on-going day-to-day business operations. Corporate Security's plan provides a measured and reasoned approach to installing new or additional security systems.

As discussed, the new physical security protection systems project is an expansion of the existing security systems blanket program included in prior GRCs. The historical blanket program expenditures of $1 million per year have been insufficient to achieve the goal of consistently deploying security systems and access controls at SCE facilities. Changes in lease agreements, growth in new facilities, and organizational changes that move personnel and operations to different facilities are also driving increased demands for adding security systems and access controls. To provide basic security protections, Corporate Security is estimating deployment at approximately 10 sites per year, prioritized based on the criticality of the site to business operations and grid reliability. Once this project has been completed, all security systems would be on a 15-year refresh cycle, commensurate with their technology obsolescence, operations, and business needs.

The continuing theft, vandalism, and damage to SCE assets underscore the need to accelerate security system deployments at locations without existing systems. These installations are also important components of an overall workplace security program to improve access control and monitoring of SCE assets and facilities, and to promote security awareness and workplace violence prevention activities and programs. The projected increase in spending is based on SCE's significantly increasing effort to deploy consistent physical protection and access controls at service centers, office buildings, regional offices, data centers, control facilities, a customer education facility, customer service facilities, and payment offices where current security systems are inadequate or non-existent.

Based on the type of location, the effort will include installation of security turnstiles, people-counting devices to improve emergency response and coordination (*e.g,* evacuation rosters and time in/outs of facilities), enterprise visitor management tools, access controls in critical areas within buildings (*e.g.*, telecom and switch gear rooms), and surveillance using close circuit television (CCTV) and other monitoring and communication systems. Accelerating the installation of new physical protection systems is a key SCE initiative to safeguard operations, information, and facilities needed for the reliable delivery of electricity and continuity of business processes on behalf of our customers.

(2) Scope

SCE is committed to the protection of personnel and assets, and supporting the continued operation of our electric facilities by mitigating internal and external security threats using security and alarm system technologies, a standardized enterprise access control system, and security monitoring and response systems integrated with the ESOC. The scope of the physical security protection system program is the acceleration of the deployment and standardization of new security systems at SCE and the correction of identified deficiencies with access control, visitor management, and monitoring of SCE entry/exit points, critical areas, and critical assets.

As part of the physical security protection system project, each security system is to be deployed based on employee population, types of protections required for differing assets, and the improvement required for identity management, access control, and surveillance. Each security system deployment will be standardized to improve management of replacement assets, maintenance costs, and 15-year refresh cycles of security technology. Each year, Corporate Security will identify the emergent threats and provide a new priority list of facilities designated for security system installations for the following year. Facilities identified for a new security system or security component will undergo a structured process to identify physical security needs and to develop a system design based on SCE security standards, installation and integration with the ESOC, and personnel training and awareness. Corporate Security will create security monitoring and response procedures for the facility based on the business needs of the respective site.

(3) Implementation Schedule

The implementation schedule is based on proactive security surveys performed by Corporate Security. The process starts at the end of the prior fiscal year when Corporate Security performs an evaluation of facilities. The evaluations are used to prioritize security

improvement projects for the next fiscal year, based on: (1) criticality to business operation, (2) the number of employees, customers, and visitors who come to the facility, and (3) the types of protection systems in place at the facility. Table II-19 below shows the project schedule.

Table II-19
New Physical Protection Systems Blanket
Project Schedule

Facility Type	2013	2014	2015	2016	2017
Service Centers	5	4	4	4	4
Office Buildings	1	8	8	8	8
Critical Infrastructure Buildings	6	5	5	5	5
Emergent Needs	2	3	3	3	3

b) Business Drivers

Corporate Security has the responsibility to protect SCE assets and personnel. Business drivers to provide the required physical protection systems are based on the operational need to protect personnel and customers from internal/external threats, and to protect SCE assets from theft, vandalism, and damage. These threats and risks can impact the safety of personnel, business operations, and the safe and reliable delivery of electricity to customers.

The original security system blanket spend of $1 million per year did not achieve the goal of deploying security systems and access controls at SCE facilities at the rate required to provide an adequate level of protection. Deficiencies identified by CRSI during the FSA process have provided the impetus to accelerate the deployment of security systems, so that SCE can reasonably protect personnel, customer, facilities, and critical assets. Changes in lease agreements, growth in new facilities, and organizational changes that move business personnel and operations to different facilities are also driving increased demands to add security systems and access controls.

c) Forecast Expenditures

Corporate Security plans to increase the forecast expenditures from the previous 2012 GRC to accelerate the installation of new security systems that allow integrated access control and monitoring of facilities and key assets at facilities lacking such systems. Table II-20 below shows the forecast expenditures by project component through 2017.

Table II-20
New Physical Protection Systems Blanket
Forecast Expenditures
(Nominal $000)

Line #	Project Component	2013	2014	2015	2016	2017
1	Corporate Security	173	346	356	365	374
2	Design and Construction	259	712	728	741	751
3	Materials	1,285	2,277	2,330	2,383	2,430
4	Installation and Test	283	763	777	792	811
5	Total (Lines 1 + 2 + 3 + 4)	2,000	4,098	4,191	4,281	4,366

d) Project Justification

The new physical protection systems project will deploy new security systems at facilities without such systems, an identified deficiency that must be addressed. SCE must take steps to limit access to facilities and key areas that can impact business operations and SCE's ability to safely and reliably deliver electricity. One key security objective that this project will address is the identification of authorized personnel for entry into a facility. Table II-21 below shows the number of annual badge deactivations and percent turnover of badged personnel for 2007-2012.

Table II-21
Badge Deactivations and Turnover of Badged Personnel

	2007	2008	2009	2010	2011	2012
Deactivated badges	1,466	1,621	1,629	1,338	2,038	3,381
Badged population	19,171	21,022	19,287	19,869	18,873	17,120
% of company badged population	7.6%	7.7%	8.4%	6.7%	10.8%	19.7%

From 2007-2012, there was an approximate 10 percent average turnover volume of badged personnel. This includes the badging and access control of vendors, contingent workers, and contractors. The high volume of turnover creates volatile lists of approved personnel who are authorized to be within SCE facilities and specific areas within facilities. Relying solely on security officers to keep up with the changes creates significant potential for errors. Without an electronic card reader to validate authorized entry, a security officer would have to make a judgment as to the person's right to

enter the facility. This is just one example of the need for technology to achieve security objectives consistently across SCE. Other security objectives also require technologies such as video surveillance and alarm and intrusion detection systems. Additionally, deploying security protection systems that can be integrated with the ESOC improves SCE's ability to detect, handle, and respond to security incidents that impact employees and visitors, customers, the public, and SCE assets.

This project addresses the gap in consistency of security measures by accelerating the installation of new physical security protection systems. More standardized physical protection systems provide cost-effective solutions that offer improved security capability for surveillance, access control, and identification of issues, reducing the need for deploying guards at all SCE facilities.

6. Security System Enhancement/Refresh (Blanket)

a) Background

The previous section addressed the need for new physical security protection systems. This section will address the need for physical security blanket funds to achieve security objectives in the many facilities with security systems (or system components) beyond their service lives or no longer operate, or operate at a degraded performance. Many of the existing security systems were deployed over 15 years ago and have antiquated technology that does not integrate with newer technologies. Older access control equipment, magnetic stripe card readers, digital video recorders, and other aged security components are outdated and no longer sold. In many cases, new wiring and mounting plates are required to integrate the modern security technology with the existing outdated security system.

The aging security infrastructure, coupled with the continuing evolution of security equipment and technologies, creates the need to perform a security refresh or enhancements to facilities with aged or poorly performing security infrastructures. This project will help maintain operational and current security systems that are compatible with computing operating systems and remain integrated with the new ESOC.

The CRSI audit performed as part of the FSAs highlighted the inconsistent deployment, maintenance, repair, and degraded operation of certain existing security systems. Many of these security systems have exceeded their service lives or no longer meet their intended purpose. Security systems functioning beyond their service lives, or that have become obsolete, are also often more expensive to maintain than to replace.

As discussed in Chapter II, Section F.5, in 2010, this project was created through the separation of the security systems blanket project into two distinct programs: one for new security systems, and a second for enhancement/refresh of existing security systems. As with the New Security Systems project, the refresh project is an expansion of the enhancements/refreshes included in the security systems blanket program in previous GRCs.[26] The original estimate of $1 million per year for both new systems and enhancement/refresh has been inadequate to achieve the goal of maintaining a proper security system refresh cycle. The limited funds were spent in a break-fix mode rather than an effective long-term plan for preventative maintenance and technology refresh. For example, many damaged or poorly operating video surveillance and intrusion detection systems have not been refreshed or maintained. As a result, some of these systems can no longer be upgraded without significant effort and will require a comprehensive security design process and system approach similar to the new physical protection system program described in Chapter II, Section F.5. The added complexity during a security system refresh involves continuing business and security operations during the security system and infrastructure refresh process.

(1) Project Overview

The purpose of the security system enhancement/refresh project is to maintain the continuing operation of monitoring systems, intrusion detection systems, and access controls at facilities (*e.g.*, service centers, office buildings, and payment offices) and their integration with the monitoring to be performed by the new ESOC. The effort will include the replacement/refresh of card readers, video recording equipment, video cameras, intrusion detection equipment and systems, people counting devices, alarm panels upgrades, alarm power supplies, security guard station equipment, and other key security system components that are used by local guard stations and the new ESOC to monitor and respond to security incidents.

Each of these security system enhancements contributes to an overall workplace security program by improving access control and monitoring of SCE access points, critical assets, and facilities while also promoting security awareness and workplace violence prevention activities and programs. SCE projects an increase in spending for security system refresh to mitigate the degraded operation of certain existing security systems, and to replace components and systems that

[26] D.09-03-025, pp. 244, 387; D.12-11-051, p. 587. *See* workpapers entitled “2009 GRC Decision Excerpts” and "2012 GRC Decision Excerpt.”

have exceeded service lives or no longer meet the intended purposes. The effort will include replacing or enhancing security turnstiles, visitor management tools, card readers, alarm panels, alarm system uninterruptable power supplies, video recorders and cameras, and intrusion detection hardware and systems.

Accelerating the security system enhancement/refresh project is essential to maintain security systems in reliable and operational conditions to address wear, obsolescence, environmental effects, and technological changes. The enhancement/refresh project is a necessary and on-going solution to maintain physical protections of key assets and facilities, provide access control for employees, customers, and visitors, and maintain operations of key monitoring systems (*e.g.*, video surveillance and alarm systems). Table II-22 below provides the 2008-2012 recorded costs and the 2013-2017 forecast for this project.

Table II-22
Security System Enhancement/Refresh (Blanket)
2009-2012 Recorded and 2013-2017 Forecast Capital Expenditures
(Nominal $000)

WBS ID	Recorded					Forecast					
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
COS-00-CS-SA-SAEP01	-	-	903	758	633	0	4,501	4,600	4,701	4,804	18,606

(2) Scope

The scope of the security system enhancement/refresh project is to maintain the operation of existing alarm, access control, and security monitoring systems at SCE. This effort includes the identification of facilities that have security systems that are non-operational or operating at a degraded performance. As part of the project, the number of covered facilities will be increased to align existing security systems with Corporate Security standards so that real-time monitoring can be achieved through the new ESOC.

As part of the security system enhancement/refresh project, we will evaluate each security system to be enhanced or refreshed based on:

- Current operations;
- How the site is being utilized;
- Types of assets requiring protection;

- Access controls based on population and types of persons at the site; and
- The required protections associated with the refresh/enhancement.

The security system refreshes or enhancements will use standardized security system equipment to improve management of replacement assets and maintenance costs, and will align with the 15-year refresh cycles for security technology. Each year, Corporate Security will identify the emergent threats and provide a new priority list of facilities designated for security systems refresh and enhancements for the following year. Each identified facility will undergo a structured review process to determine security needs based on SCE security standards, installation and integration with the new ESOC, and personnel training and awareness. Corporate Security will create security monitoring and response procedures based on the business needs of the respective site.

(3) Implementation Schedule

The implementation schedule for security system refresh or enhancements is based on proactive security surveys performed by Corporate Security at the end of the prior fiscal year. The data is used to prioritize the next fiscal year's security improvement projects based on the service life of the security system, operational performance of the existing system, criticality to business operations, number of employees, customers, and visitors that work at or visit the facility, and the types of systems currently deployed at the site. Table II-23 below shows the implementation schedule for the security system refresh and enhancements by facility type through 2017.

Table II-23
Security System Enhancement/Refresh
Implementation Schedule

Facility Type	2013	2014	2015	2016	2017
Service Centers	0	4	4	4	4
Office Buildings	0	8	8	8	8
Critical Infrastructure Buildings	0	5	5	5	5
Emergent Needs	0	3	3	3	3

a) Business Drivers

Many existing security systems and their components are past their expected 15-year service life.[27] The continuing need to protect personnel and customers from internal/external threats and protect SCE assets from theft, vandalism, and damage drives this project. The risks inherent in an aging security infrastructure, equipment obsolescence, and degraded security equipment performance threaten the safety of personnel, customers, and the public and the safe and reliable delivery of electricity to customers.

The original security system project spend of $1 million per year, which included the New Physical Security Protection Systems project discussed in Chapter II, Section F.5, did not achieve the goal of maintaining security systems and access controls at SCE facilities at the rate required to provide adequate levels of protection. Deficiencies identified by CRSI as part of the FSAs have provided the impetus to accelerate the refresh and enhancement of existing security systems so that SCE can provide security protections to personnel, customer, facilities and critical assets. Changes in lease agreements, growth in new facilities, and organizational changes that move business personnel and operations to different facilities are also driving increased demands in refreshing security systems and access controls.

b) Forecast Expenditures

Table II-24 below shows the forecast expenditures by project component through 2017.

[27] Based on the hundreds of cameras and card readers that are no longer manufactured or serviceable, we estimate that approximately 30 percent of systems and/or components are past their 15-year service lives.

Table II-24
Security System Enhancement/Refresh (Blanket)
Forecast Expenditures
(Nominal $000)

Line	Project Component	2013	2014	2015	2016	2017
1	Corporate Security	0	420	431	442	453
2	Design and Construction	0	578	589	595	601
3	Materials	0	2,713	2,775	2,843	2,909
4	Installation and Test	0	789	805	821	841
5	Total (Lines 1 + 2 + 3 + 4)	0	4,500	4,600	4,701	4,804

c) Project Justification

Maintaining the operation of the existing security protection systems is critical to SCE's ability to identify and respond to security threats, risks, and incidents. The aging security infrastructure will make it difficult to maintain the integration of security alarms with the new ESOC and will impact our ability to detect, handle, and respond to security incidents. Additionally, security systems functioning beyond service lives or that have become obsolete are often more expensive to maintain than to replace. Unexpected malfunctions caused by the age of equipment can also lead to increased security guard expenses to address security gaps while malfunctioning equipment is repaired or replaced.

7. A-Substation Security Perimeter Improvements (Blanket)

a) Background

The A-Substation security perimeter improvements (blanket) project continues the process of ongoing improvements to the perimeters of A-Bank stations that began in 2009. This project was first authorized in the 2009 GRC decision but was put on hold for the 2012 GRC as SCE assessed security requirements for NERC CIP compliance.[28] The request for funding for this blanket project was made by T&D in the 2009 GRC application. Going forward, Corporate Security will request funding for this project directly.

As part of an on-going effort to improve the reliability of the BES, between 2009 and 2012, SCE deployed physical security improvements at 12 A-bank substations. Whereas NERC

[28] D.09-03-025, p. 224. *See* workpaper entitled "2009 GRC Decision Excerpt."

CIP compliance efforts address only the protection of BES cyber assets, which is the focus of the NERC CIP Standards, the A-substation security improvements project has a broader focus. The project addresses public safety and the security of the overall facility, not just BES cyber assets located at the facility. This program seeks to improve the protection of electrical equipment, buildings, and people by hardening fence lines, improving gate and door access controls, and adding intrusion detection and video surveillance.

Electrical power to our customers is provided through a complex network of wires and substations. There are three general substation categories: (1) AA-Bank, or 500kV substations, (2) A-Bank, or 220kV substations, and (3) B-Bank, which are generally referred to as distribution substations. Regardless of category, each of these substations has security features, such as perimeter fencing, access controls using keys or electronic card readers, and alarm systems wired to the interior substation control rooms. These security measures provide our substations with basic levels of protection against intruders. These measures also protect the general public from energized substation equipment, which can be lethal.

AA-Bank substations are often used as bases for the deployment of transmission crews, trucks, and equipment. Most 500kV AA-Bank substations are staffed due to the large amount of equipment in use at these stations. The loss of a single AA-Bank substation can disrupt electric service to over 600,000 customers and potentially cause stability problems to the overall SCE electrical system. Thus, all AA-bank stations have physical security measures integrated into the current CAS monitoring system. The baseline security features for AA-bank substations include perimeter intrusion detection, alarming of specialized areas and equipment, access control at buildings and gates, and remote video surveillance equipment.

Unlike AA-Bank substations, the 220kV A-Bank substations are, with few exceptions, generally not staffed. The loss of an A-Bank substation can disrupt electric service to over 100,000 customers, and can potentially also cause stability problems to portions of SCE's electrical system. Many of these stations are in very remote locations and have been equipped with automation to allow the substation equipment to be remotely controlled from regional Switching Centers. The use of automation has allowed the Switching Centers to operate more efficiently and to coordinate the activities of many A-Bank substations with fewer personnel. Most of the 220kV substations do not have security systems that monitor security perimeters, building access, or gate access. These substations use video surveillance equipment similar to the AA-bank stations.

(1) Project Overview

As of year-end 2012, SCE has completed video surveillance enhancements at 12 facilities.[29] Ongoing incidents of theft, vandalism, and damage to the generally unstaffed A-Bank substations continue to present a significant risk and disruption to SCE's operations. Each incident of theft, vandalism, or damage involving an A-Bank substation requires T&D crews to coordinate with Grid Operations, Engineering, and Substation Maintenance crews to shift resources and power to perform repairs. Additionally, power outages to customers are common while repairs are being completed. Table II-25 below lists the recorded expenditures between 2009 and 2012, as well as the 2013 to 2017 forecast, for the A-Bank substation perimeter security project.

Table II-25
A-Bank Substation Perimeter Security
2009 – 2012 Recorded and 2013 – 2017 Forecast Expenses
(Nominal $000)

WBS ID	Recorded					Forecast					
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
COS-00-CS-CS-ASUBS	-	2,015	3,201	2,221	7	2,200	2,249	2,300	2,350	2,397	11,496

We will continue to deploy physical security improvements at A-Bank substations to mitigate the impact on service to customers resulting from instances of theft, vandalism, and damage at A-Bank substations. These improvements include the deployment of video surveillance and intrusion detection equipment at substation perimeters, access controls at gates and buildings, improved intrusion detection at building perimeters and key assets within the substation, and integration of alarm monitoring and response with the new ESOC. These improvements provide appropriate levels of deterrence and physical security measures to improve the identification of and responses to potential theft, threats, vandalism, or damage at or to A-Bank substations, each of which has the potential to immediately impact the delivery of electricity to 100,000 customers.

(2) Scope

SCE plans to spend $11.496 million from 2013-2017 to complete the installation of security systems at three 220kV substations per year. The substation security improvements will encompass physical protections of the building and critical areas, additions of

[29] *See* workpaper entitled "A-substation Security Improvements Historical Details."

perimeter intrusion detection at the fence lines and buildings, integrated access control and alarm management with the ESOC, and video surveillance improvements. The number of installations that can be completed during this period is limited by the amount of available resources, both human and physical. Thereafter, SCE intends to spend an additional $2.4 million per year from 2018 through 2023 to complete upgrades at the remaining 220kV substations that will not yet have video surveillance perimeter intrusion detection systems. These additional future expenditures are not included in this GRC request.

(3) Implementation Schedule

The implementation schedule is based on a joint approach with T&D's Grid Operations and Corporate Security. Each of the 42 additional substations has been ranked in order of impact to the BES, recurrence of issues and threats to the facility, and current security conditions at each site. Corporate Security plans to complete security system installations at three substations per year from 2013 through 2017, for a total of 15 substations during this period. This is consistent with historical project performance in which installations were completed at 12 substations from 2009-2012, an average of three per year.

b) Business Drivers

The need for ongoing improvement of physical security at A-Bank substations is driven by continuing incidents of theft, vandalism, and damage to or at A-Bank substations, some repeatedly, as well as their critical importance to the reliable delivery of electricity to customers. Additionally, the threats and risks can impact public safety if an unauthorized individual enters these energized facilities. The security monitoring and deterrence deficiencies, as well as the very remote location of many of the A-Bank substations, increase the potential for unauthorized entry and malicious activity at A-Bank substations. Improving the physical protection systems at the A-Bank substations continues to be an important SCE initiative to actively safeguard key systems, information, and facilities necessary for the reliable delivery of electricity and continuity of business operations.

c) Forecast Expenditures

Corporate Security plans to install security improvement at three A-Bank substations per year during 2013-2017. Table II-26 below provides the recorded and forecast average cost per substation.

Table II-26
A-Substation Security Perimeter Improvements
Average Cost per Substation
2009-2012 Recorded and 2013-2017 Forecast Expenses
(Nominal $000)

	Recorded	Forecast				
	2009-2012	2013	2014	2015	2016	2017
Cost-per-substation	620	733	750	767	783	799

Table II-27 below shows the distribution among various OUs of the costs to implement the security perimeter improvements for 2013- 2017.

Table II-27
A-Substation Security Perimeter Improvements
Forecast Expenditures
(Nominal $000)

Line #	Project Component	2013	2014	2015	2016	2017
1	Corporate Security	205	208	213	218	224
2	T&D Design and Construction	282	311	319	327	335
3	IT Telecon	323	323	330	336	343
4	Materials	741	750	769	786	799
5	Installation and Test	647	657	670	683	697
6	Total (Lines 1 + 2 + 3 + 4 +5)	2,198	2,249	2,301	2,350	2,398

d) Project Justification

As an alternative to video surveillance or other type of technology, SCE could use 24-hour guard service at each of the 42 A-Bank substations. For the larger substations, guards posted outside the perimeter fence are hindered in their ability to monitor the site by the sheer size of the substation. Guard service at substations also is problematic due to the low pay and high turnover generally associated with these types of services industry-wide. As noted by the Service Employees International Union:

> A recent report on the private security services industry in the U.S. estimates that annual employee turnover in our industry still exceeds 100

> percent for many security companies and can be as high as 300 to 400 percent for low-road firms. These turnover rates rival those of the fast food industry and pose a serious risk to public safety as private security officers often are first responders to life-threatening emergencies.[30]

High turnover rates would add to the operational difficulty of providing safety training to these personnel, and make it extremely difficult to maintain a pool of guards who have proper substation training and can safely access a substation. Security guards generally are not trained to operate near high-voltage substation equipment, which means the guards could not enter if they are not properly trained on the hazards associated with substation equipment.

The business need to protect A-Bank substations is based on the continued operations of the substations and reducing the potential of an electrical outage to 100,000 customers or more at a time. The lack of integrated security monitoring with the ESOC further increases the risk of delayed response times and our ability to prevent theft, vandalism, and damage to A-Bank substations. On balance, given the cost for a non-technology solution, and the reliability and safety issues associated with that option, the intrusion detection and video surveillance system will better serve the goal of improving A-Bank substation security.

---

[30] *See* workpaper entitled "SEIU Our Industry – Private Security."

III.

BUSINESS RESILIENCY

A. Overview and Summary of Test Year Forecast

SCE's 2015 O&M expense forecast for the Business Resiliency department is $4 million, an increase of $1.792 million above 2012 recorded expenses. This increase is primarily driven by strategic improvements needed in SCE's business resiliency planning and emergency management activities. Specifically, Business Resiliency is implementing a new, outward-facing, all-hazards approach to business resiliency. This new approach will help align SCE's recovery strategy and plans with those of federal, state, county, and community agencies, which will permit a more coordinated, effective, and efficient recovery from future emergencies and disasters. One key aspect of this strategy is the need to substantially increase joint planning and training between and among SCE's Operating Units (OUs) as well as with public sector emergency agencies.

B. Overview of Business Resiliency

Business Resiliency's two fundamental responsibilities have been supporting the continuity of critical internal processes under abnormal conditions, and helping manage SCE's emergency planning and response – to avoid or minimize service disruptions, harm to individuals, and damage to assets. Several watershed events in recent years, however, have taught us that we need to fundamentally alter the mission of our organization by deepening our focus and broadening our scope to mitigate the impact of extreme emergencies on the company and the communities we serve.

Recently, the department has been focused on improving our internal business continuity and emergency response planning to better position SCE to respond to localized and/or common emergencies. Going forward, SCE will actively address an identified gap in our planning: responding to an extreme natural or man-made disaster on a regional scale. It has become increasingly clear to SCE that extreme emergencies create systemic crises for communities and metropolitan areas, not just increased numbers of isolated problems. Extreme emergencies and catastrophic events are qualitatively different than most emergencies with which SCE has direct experience. We have learned that emergency planning in isolation—however well done—will not result in the most efficient restoration of service that our communities will need from us following a future catastrophic event.

1. Lessons Learned from Direct Experience and Benchmarking

SCE has learned from its experience in responding to emergencies affecting the company's service area, and supporting other utilities in their response to emergencies outside of our service area, as well as benchmarking and studies of disasters around the world.

In particular, on November 30, 2011, Southern California experienced a severe wind storm causing significant electrical system damage in the San Gabriel Valley area and interrupting electric service to over 400,000 customers. The storm damage led to power outages to some customers for up to seven days. Our response to this event was not satisfactory. As a result of our post-event assessment, an independent evaluation performed by Davies Consulting, feedback from public participation hearings, and a report by the California Public Utility Commission's (CPUC) Consumer Protection and Safety Division (now Safety Enforcement Division), we identified a number of areas that needed improvement.[31]

SCE also learned important lessons from Hurricane Sandy. When that storm hit the Northeast in October of 2012, it effectively shut down whole states along the entire East Coast. Over 8.2 million customers lost power. The nation observed the cascading consequences of power failure on critical community services and commerce. SCE sent mutual assistance crews, equipment, and Business Resiliency's emergency management team to support restoration in hard-hit New York. In doing so, we saw first-hand evidence of successful utility/public agency partnerships in preparing for such an event.

For example, as a result of clear mutual understanding and real time communication between Consolidated Edison of New York and public agencies, ConEd was able to make the remarkable decision to de-energize much of Lower Manhattan temporarily to prevent serious damage to the underground grid due to flooding. The temporary outage, while a serious short term consequence, protected the system from damage that would have created extended outages and costly, long term restoration. This decision could not have been made, or implemented, without clear communications and coordination between ConEd and public agencies.

These experiences, supported by extensive research and benchmarking, revealed common characteristics of successful and unsuccessful responses to extreme or catastrophic disasters. In each case, successful outcomes resulted from deliberate, pre-event collaborative planning between the electric

---

[31] *See* workpapers entitled "Final Report, Southern California Edison's Response to the November 30, 2011 Windstorm" (Davies Report) and "Investigation of Southern California Edison Company's Outages of November 30 and December 1, 2011 Final Report" (CPUC Report).

utility and public sector emergency management agencies at all levels, as well as with other critical infrastructure providers in lifeline sectors such as food, agriculture, transportation and financial services.

2. Increasing the Focus on Business Resiliency at SCE

Acting on this new insight, SCE has begun to make many changes to its business resiliency organization, strategy, processes, and procedures to improve our planning, response, and recovery activities. One major organizational change was separating critical business resiliency planning and preparedness functions from the Corporate Security department by elevating Business Resiliency to a department within the Safety, Security, and Compliance (SS&C) OU. This department reports directly to the Vice President of SS&C. Business Resiliency is now building and implementing a new model for emergency planning and execution that is both broader in scope and deeper in focus. The new model includes:

- Revising the processes and procedures in the Corporate Emergency Response Plan (CERP);
- Implementing the National Incident Management System (NIMS) of which the Incident Command System (ICS) is a part;
- Expanding the scope of drills to include joint exercises conducted with and evaluated by public sector responders, communities and customers performing vital functions;
- Increasing our investment in technologies, facilities, and equipment; and
- Preparing to take an active role, including a leadership role, in a "whole community response" to large-scale outages and other emergency situations.

A second major step was a nationwide search for a Director with specific experience in federal emergency management. As a result of that search, in early 2013, I joined SCE as the Director of the Business Resiliency department to build on the strong foundation already achieved by the department and introduce a new level of value to customers and the public. I have 30 years of experience in national security and emergency management, including 26 years of service in the federal government with the Federal Emergency Management Agency (FEMA), the Department of Energy, the Environmental Protection Agency, and the Department of Defense. Immediately prior to joining SCE, I was FEMA's Director of Response.[32]

[32] Additional information regarding my background and experience is set forth in Appendix A.

Since my arrival, we have carefully assessed the work and the organization of the department. Based on my background in emergency management, emergency operations, and emergency planning, I worked with the department's existing staff to outline the specific new work necessary for SCE to address the areas of improvement identified by our post-wind storm assessment, the Davies Report, and the CPUC Report. The new work will allow SCE to better plan for and respond to the wide range of emergencies that can impact SCE's ability to provide safe and reliable electricity to the communities we serve.

This new work, characterized by an all-hazards approach to joint planning between the public sector and the private sector, is designed to align SCE's planning with the response and recovery approach used by public sector emergency agencies at the local, state, and federal levels. This type of integration will help SCE fulfill the responsibility of critical infrastructure providers set forth in public policy and planning documents, including NIMS, the Critical Infrastructure Protection Plan, the Southern California Catastrophic Earthquake Response Plan, and other public sector plans and strategies.

This is not merely policy or theory. At the boots-on-the-ground restoration level, this approach contributes to improved public safety, better organized restoration of electric and other critical services, and less disruption of local business and traffic flow. For example, if downed trees must be cleared and damaged poles must be replaced in a neighborhood, it makes sense for all service providers to coordinate their restoration work in the safest, quickest, and most cost-effective manner. This coordinated, tactical approach to restoration includes, for example, coordination among SCE, natural gas services, telecommunications and cable providers who share our poles, and public works services such as debris removal, water distribution, sewer systems, tree trimming, traffic lights, detours, and curfews.

3. Scope and Objectives of the New Business Resiliency Department

The testimony below details how the increased funding will help SCE—as the provider of a fundamental lifeline service—improve resiliency. The testimony will address three broad objectives of the new Business Resiliency Department that drive the SCE request. They are:

- Governance – Building a leadership and accountability structure to identify and systematically resolve internal and external preparedness gaps and to integrate SCE's internal readiness activities into a new community resiliency model;
- Plans and Programs – Augmenting the existing planning and plan management capacity through incremental staffing, training, and by acquiring a dedicated business

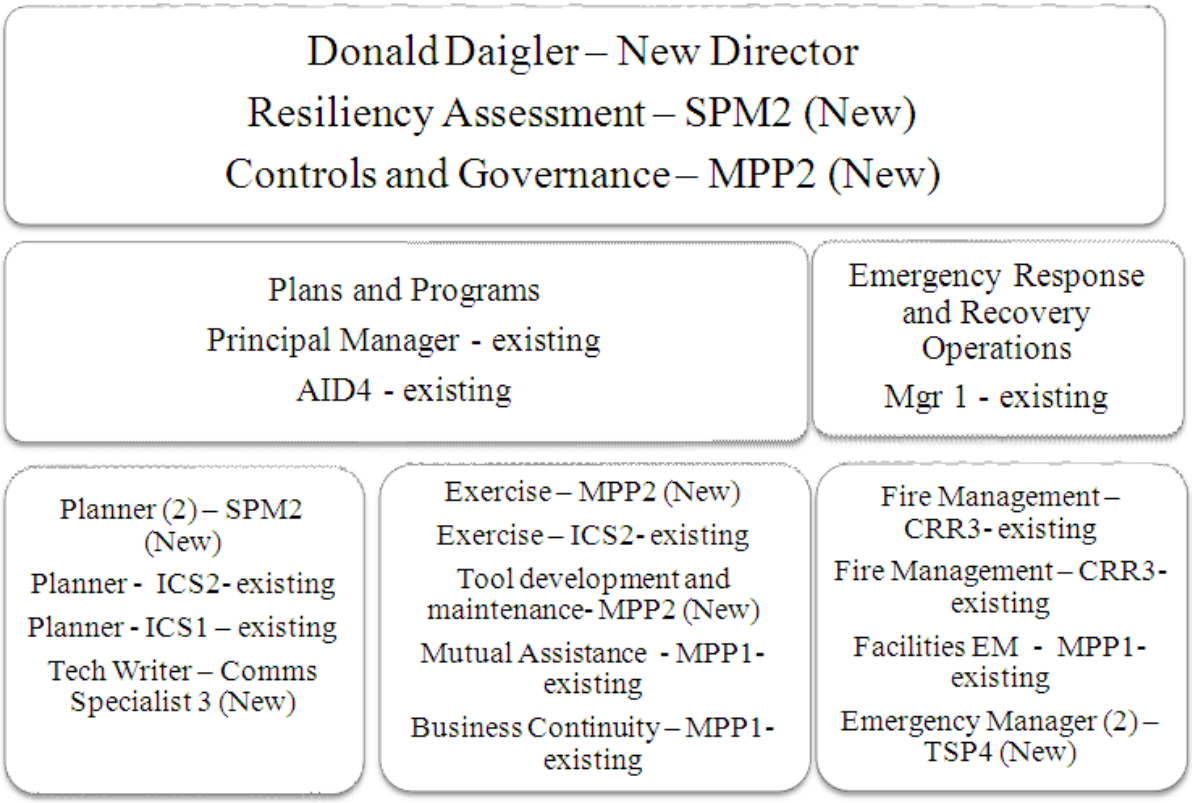
resiliency information management tool. This objective includes joint exercises and training which will broaden existing training, planning, and exercise programs by including more joint exercises with public agencies, other utilities, and other community agencies; and

- Emergency Response and Recovery Operations – Substantially increasing SCE's emergency response and management capacity using NIMS, of which ICS is a part, to improve community-wide recovery from emergency conditions.[33]

Business Resiliency's success depends on its specialized professional personnel. As such, a majority of the O&M increase is to permit the addition of ten specialized personnel (including a director) to augment a small existing staff of eleven. This larger organization will continue ongoing work while taking on the new challenges inherent in the three objectives described above. The reorganization of the department, including the number and quality of the staff for the department, is based on my knowledge and experience, including my having performed and/or supervised those performing each of the positions/functions described below. As a result of my experience, I am intimately familiar with the knowledge and experience required for these positions, the number of hours required to fulfill the functions, and the number of personnel required to properly execute the duties and responsibilities of those positions. The organization of the new Business Resiliency department is detailed in Figure III-7 below.

[33] As described by FEMA, NIMS "identifies concepts and principles that answer how to manage emergencies from preparedness to recovery regardless of their cause, size, location or complexity. NIMS provides a consistent, nationwide approach and vocabulary for multiple agencies or jurisdictions to work together to build, sustain and deliver the core capabilities needed to achieve a secure and resilient nation." (http://www.fema.gov/national-incident-management-system). FEMA describes ICS as "a standardized, on-scene, all-hazards incident management approach that: Allows for the integration of facilities, equipment, personnel, procedures and communications operating within a common organizational structure[;] Enables a coordinated response among various jurisdictions and functional agencies, both public and private[; and] Establishes common processes for planning and managing resources." (http://www.fema.gov/incident-command-system).

Figure III-7
Business Resiliency
Organization Chart



The increased staffing and the functions to be carried out by the reorganized department described above reflect the minimum changes needed for Business Resiliency to put in place the necessary processes and plans for SCE to effectively respond to most emergencies.

Another important area of focus for the department is improving the accessibility of information for Business Resiliency personnel – both to inform planning activities and support operational decision making during response and recovery operations. This information includes: (1) plans, forecast models, dashboards, and situational awareness data, (2) the technology to acquire, store, maintain, and display the information when needed, and (3) the technical personnel required to make optimal use of the information.

C. Forecast of Incremental O&M Expenses

The three objectives introduced above will be achieved with incremental annual O&M expense of $558,000 in non-labor and $1.235 million in labor. The components comprising these expenses are discussed below.

1. Resiliency Governance

O&M expenses of $463,000 are required to implement the new leadership necessary to operate Business Resiliency as an independent organization with its new and broadened scope of work. The leadership model being implemented recognizes the criticality of reliable electric service to community interests as well as to national security and economic health. The addition of the following annual salaries/expenses will permit Business Resiliency to meet its broader and expanded goals: (1) Director's salary of $150,000 and expenses of $15,000, (2) a Strategic Planning Manager, Level 2 (SPM2), at $129,000, (3) a Program/Project Manager, Level 2 (MPP2), at $124,000, and (4) $45,000 in professional development costs.

We will begin with a comprehensive assessment of SCE's current level of resiliency, based on standard measures of the contributors to successful emergency preparedness, scalable response, and community-wide recovery. This assessment will measure SCE's readiness for specific scenarios as well as general, non-specific emergencies. It will also provide executive management with a clearer understanding of corporate readiness within the larger context of public sector response and recovery protocols.

As part of this assessment, we will develop a business resiliency strategy and governance model. The strategy will focus on all-hazards planning across the entire spectrum of business resiliency practices from assessments, through emergency management, planning, restoration, and recovery, to fully functional exercises that are scored against nationally accepted criteria and conducted jointly with first responders, government agencies, and other critical partners.

The Director, Strategic Planning Manager, and Program/Project Manager positions will provide the necessary leadership for the department. With my leadership team, Business Resiliency will be able to implement the necessary improvements to help the department meet the objectives and goals outlined above.

The MPP2 position will focus on integrating SCE Business Resiliency risk assessment and planning models with public sector response and recovery programs, including critical infrastructure, key resource, and sector-specific plans. Opportunities exist for SCE to integrate its plans

with existing plans at the local, state, and county levels, which will allow SCE and the public sector agencies to communicate effectively, coordinate resource deployment according to shared priorities for maximum efficiency, and to improve the safety of the public and those responsible for recovery. This position will require national level business resiliency training and experience.

One simple example of effective communication and coordination is dealing with fallen trees and downed wires that have blocked streets following an event. These conditions limit emergency personnel's access to the affected area and create a dangerous situation for the public. SCE, communities, counties, and the state all have resources that need to be deployed to clear the streets. Coordinated planning and communication will help to deploy resources in the most efficient manner. The coordinated response will be prioritized to clear the most critical streets first. The affected lines will be de-energized so that it is safe for the responders to work when they get there. This type of coordination will help prevent situations that occurred in the 2011 windstorm, where tree clearing crews showed up on one street, only to wait an hour for the lines to be de-energized by an electrical restoration crew waiting on a different street for the trees on that street to be cleared.

The work that needs to be done on an ongoing basis includes:

- Regularly conducting comprehensive assessments of SCE's readiness for emergencies at all levels;
- Establishing and maintaining critical external relationships and strategic partnerships with federal, state, county and city government emergency management entities, emergency responders, and customers providing critical services;
- Developing and overseeing initiatives that integrate SCE's resiliency plans with those of existing plans at the local, state and county levels; and
- Monitoring and improving the strategy and governance model based on metrics, drills, benchmarking, and actual events.

In addition to these functions, the MPP2 position will address a number of the recommendations set out in the Davies Report.[34]

Examples of public sector plans for preparedness, prevention, response and recovery with which SCE will become better integrated as a result of this position include:

---

[34] *See* Davies Report, recommendations EPP1, EPP9-10, and C6.

- Operational Area (county) emergency plans for the 13 California counties within the SCE service territory;
- The State of California Emergency Plan 2009;
- The Southern California Catastrophic Earthquake Response Plan;
- The National Incident Management System, 2008;
- The National Infrastructure Protection Plan (NIPP);
- NIPP Annex: Energy Sector-Specific Plan, 2010;
- NIPP Annex: Dams Sector Specific Plan, 2010;
- National Disaster Recovery Framework, 2011;
- Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection";
- Homeland Security Presidential Directive 8, "National Preparedness"; and
- US Department of Health and Human Services Pandemic Influenza Plan and corresponding state and county public health plans and protocols.

The SPM2 position will be responsible for developing specific, measurable, attainable, and timely metrics and controls for Business Resiliency. These metrics will establish internal controls by which the efficacy of the program may be measured. They will also create the governance model used to track and measure the activities of the OUs in emergency response, process recovery, and exercise success. The work of this position includes:

- Monitoring compliance with program processes and procedures;
- Reporting on status of planning, response, exercise goals;
- Overseeing the creation of educational material for the OUs explaining the governance and control processes; and
- Monitoring crisis team exercises to identify action areas.

a) Staff Development/Professional Associations

The field of Business Resiliency is constantly evolving. Every new disaster anywhere in the world provides lessons that can be applied to improve SCE's planning and readiness. Scientific advances in many fields often provide better tools and models to be used for forecasting the behavior of events that may affect electrical infrastructure. Better models mean better preparedness. Degrees and certifications in emergency planning, hazard mitigation, exercise planning and evaluation, and emergency management, among others, are offered by FEMA, California Emergency Management

Agency (CALEMA), and local universities. Additionally, professional organizations and groups provide a forum for exchanging best practices and lessons learned from events. So that SCE personnel can stay abreast of relevant developments in the business resiliency/emergency preparedness field, and take advantage of information available through professional organizations, we forecast $45,000 in non-labor O&M expenses for staff development. The importance of continued professional development and the acquiring of relevant certifications were among the recommendations in the Davies Report.[35]

2. Plans and Programs

SCE must strengthen its existing internal and external planning and plan management capacity through incremental staffing, training, and by acquiring a dedicated business resiliency information management tool. SCE is forecasting incremental 2015 O&M expense of $1.012 million to fund this expanded capacity. This forecast includes: (1) a new centralized planning tool recommended in the Davies Report ($112,000),[36] (2) two new Strategic Planning Manager, Level 2 (SPM2) positions at $129,000 each, (3) a Communications Specialist, Level 3(CS3) position at $101,000, (4) two Program/Project Manager, Level 2 (MPP2) at $124,000 each, and (5) $293,000 for outside training consultants. The need for the tool and these positions is discussed below.

a) Centralize and Strengthen Planning

Business continuity planning is an on-going cycle of Business Impact Analyses (BIA), developing and updating plans, and conducting exercises. A BIA identifies and prioritizes business processes and the impact if the process is interrupted. Before preparing a plan to recover the process, a recovery strategy is defined to mitigate, remediate, or accept the risk posed by interruption of the process. Planning then identifies approaches to avoid or minimize these interruptions, and steps to take if they do occur. During this stage, planners also examine critical supply lines and alternative resources for the resumption of critical functions as quickly as possible.

Currently, Business Resiliency coordinates with other OUs to guide them through the planning process. The management and maintenance of the plans has been the responsibility of the individual OUs. As a result, business continuity planning can be fragmented and inconsistent among SCE OUs. For example, recovery strategies are formulated by people unfamiliar with the range and scope of available mitigation and remediation possibilities. And risks that are accepted by an OU are

---

35 *See* Davies Report, Recommendation EPP8.

36 *See* Davies Report, Recommendation EPP3 and EPP11.

not documented in a manner visible to other OUs or to Business Resiliency. Continuity plans, although based on a single template, are written with varying degrees of rigor, depending on the knowledge and experience of the OU resource assigned to the task. For many, the assignment to maintain the OU's continuity plan is an ancillary duty, and not something to which they can devote much time. To address this issue, with the input of OU subject matter experts, Business Resiliency will assume this planning responsibility on a company-wide basis. Under this approach, business continuity planning will be done by personnel trained in planning and plan integration at the national level. The OUs will be relieved of the need to develop expertise in creating and maintaining plans, and will be able to focus their resiliency efforts on providing the subject matter expertise needed to create robust company-wide recovery plans.

To implement this change in the continuity planning process, the current two-person planning staff previously tasked with working with OUs needs to be augmented with two additional Strategic Planning Managers, Level 2 (SPM2s), at an annual cost of $129,000 for each position. These SPM2s will be responsible for:

- Standardizing operational recovery planning at SCE;
- Creating, maintaining, and rolling out a consistent model for executing all facets of the business resiliency planning lifecycle, including the new responsibility of supporting the OUs;
- Providing strategic direction in the development of policies, repeatable processes, procedures, templates, job aids, training materials, checklists, and handbooks;
- Coordinating with subject matter experts across SCE – such as Grid Operations, Distribution, Corporate Communications, Customer Service, and Local Public Affairs – to develop, maintain, exercise, and integrate continuity and emergency response plans;
- Engaging with public sector emergency agencies (federal, state, county, and local) to improve coordination during emergencies through collaborative planning, building interoperability through information exchange, and joint exercises. This new body of community-facing work will better integrate and synchronize response and recovery activities between SCE and public sector emergency agencies;

- Expanding the focus of planning beyond storms to include any incident that can impact the electrical grid or SCE's ability to perform critical business functions; and
- Collaborating with OUs and leadership to develop success metrics, compile risk logs, assess progress, and address identified gaps.

These positions and their functions will address the Davies Report recommendations relating to plan preparations.[37]

b) Standardize Communication and Documentation

Clear communication is critical to continuity and interoperability between and among SCE's emergency management and business continuity plans, including plans for electrical restoration, and those of external critical infrastructure planning partners. Consistent and mutually understood terminology and documentation based on the ICS model will contribute to efficient, accurate, and timely communication between the utility and public agencies. We will achieve this by developing and maintaining policies, repeatable processes, procedures, templates, job aids, training materials, checklists, and handbooks using standard vocabulary.

This new function will be performed by a Communication Specialist, Level 3 (CS), at an annual cost of $101,000. The CS3 position will also reach out to external planning partners to obtain and disseminate relevant documentation to foster mutually understandable vocabulary, directives, and constraints.

c) Business Resiliency Information Management System (BRIMS)

Business Resiliency is requesting $112,000 in incremental O&M expense for annual licensing and hosting fees associated with a new business resiliency information management system (BRIMS) planned for implementation in 2013.[38] BRIMS will improve the quality and accuracy of the emergency and business continuity plans that will be maintained within the system, while at the same time simplifying the plan management process. Specifically, BRIMS will:

- Automate the maintenance of contact information in emergency plans, minimizing the risk of costly and error-prone manual maintenance of multiple plans;

---

[37] *See* Davies Report, Emergency Planning and Preparedness Recommendations and RE1 through RE4.

[38] *See* workpaper entitled "BRIMS Estimate."

- Identify dependencies among internal business processes to prioritize restoration efforts and determine the sequence in which processes should be restored;
- Derive personnel training and qualifications directly from the Human Resources database system to provide a roster of personnel able to fulfill roles in an emergency that are outside of their normal duties (Secondary Job Roster) and to verify that all employees with roles in emergency management or business continuity planning are properly prepared and trained for those roles;
- Automate the tracking of exercise action items as well as any new issues or challenges identified during the exercise process; and
- House questionnaires and OU responses used to prioritize restoration efforts and business function resource requirements.

Data easily derived from reports created in BRIMS will enable better decision-making regarding where to spend resiliency dollars for the greatest impact in mitigating risks for the entire company. BRIMS will also increase the efficiency of governance functions by tracking updates and providing Work Flow capabilities, which will help confirm that plans are updated in a timely fashion and will support timely review and approval of updated information.

d) Joint Exercises and Training

Business Resiliency is estimating $541,000 in incremental O&M expense to broaden the existing training and exercise program to support the integration of public sector agencies and other external parties. This request is for two new Manager, Program/Project, Level 2 (MPP2) positions at $124,000 each per year and $293,000 for outside training consultants.

SCE regularly participates in and conducts training sessions and exercises to identify gaps in planning, processes, methodologies, or resources, as well as to prepare SCE employees and other parties to respond in an emergency. The scope and depth of these exercises will be broadened to include all hazard situations, multiple agency interfaces, strategic and tactical planning using ICS, deployment and tracking of large numbers of resources both for restoration and support, and use of technologies developed for plan synchronization, situational awareness, and decision support.

One incremental resource, a Manager, Program/Project is required for broadening the training and exercise program to support the integration of public sector agencies and other external

parties. This position requires someone with training and experience at the national level in managing large scale exercises involving both private and public entities.

Specific responsibilities of this new position include:

- Refining and maturing exercise processes, procedures, and evaluating methodology, and training materials;
- Aligning the exercise process with those of public sector response entities
- Training and testing scenarios involving mutual assistance;
- Managing joint exercise across the company and public sector response entities;
- Managing remediation of issues identified in exercises and drills; and
- Managing NIMS/ICS course development, training and exercises.

Another Manager, Program/Project, is required for developing and maintaining situational awareness and decision support tools. To make good decisions in an emergency, it is necessary to have as much information as possible regarding the situation and the status of recovery efforts. To coordinate and prioritize efforts across the whole of the incident, the various groups and agencies involved in the recovery need to be able to share information. This MPP2 will work with public sector emergency management teams to determine what information they use or create in an emergency, to determine what information they need from SCE in an emergency, and to facilitate the effective sharing of data. This position will also work with scientists and technology experts to determine the availability of information concerning the SCE service territory that will help us predict or manage emergencies. This position will also manage the design, development, and optimization of BRIMS, as well as other internal analytical tools to automate governance, reporting, and plan integration, and to provide the real time situational awareness necessary to manage emergency operations effectively.

Specifically, the MPP2 will be responsible for:

- Developing requirements and business case for technology improvements
- Developing dashboards and predictive models;
- Monitoring the maturation of the tools, and ensuring full utilization of tool features;
- Developing metrics and reports that accurately reflect the effectiveness of the Business Resiliency program;

- Reviewing and recommending improvements based on lessons learned from events, drills, benchmarking, metrics, and reporting;
- Achieve data integration with other corporate systems, such as SAP;
- Evaluating risks and resolving issues with data integration and usage;
- Determining the availability and accessibility of necessary information;
- Staying abreast of research and technical advancements that increase accuracy of existing information, or create new information; and
- Creating and maintaining tools to analyze information and present it in a format that is usable by internal Emergency Managers as well by public sector emergency managers.

In addition to the above described staffing increases, SCE also estimates $293,000 in costs to retain professional outside services to revise and deliver ICS training, to develop emergency scenarios, and to conduct exercises and practical application workshops. Access to this external expertise will further SCE's on-going efforts to improve its ability to respond to emergencies in close coordination with public agencies and other utilities. By fully adopting the NIMS methodology, including ICS, SCE will use the same language, organizational principles, and reporting channels used by FEMA, CALEMA, local municipalities, and first responders.

Increasing the number of trained individuals will improve our restoration capability, enable us to communicate and interface effectively with local emergency personnel, and provide sufficient resources to staff an emergency around the clock. SCE currently has sufficient trained personnel for four shifts of emergency management per day. While this may appear to be adequate, additional trained staff are necessary because staff trained for a particular position may not be available for every incident (*e.g.*, health or personal issues may prevent attendance). Additionally, multiple incidents occurring simultaneously may also require trained personnel to be available on a standby basis.

3. Emergency Response and Recovery Operations

Business Resiliency estimates $319,000 in incremental O&M expense to substantially increase SCE's emergency response and readiness capacity to improve community-wide recovery from emergency conditions.

a) Emergency Management Personnel

Existing Emergency Managers provide subject matter expertise and direct support to OUs for all emergency management functions. Emergency managers currently assist in disaster cadre

development (curriculum development and validation) for emergency management functions. Business Resiliency requires two additional Emergency Managers (Technical Specialist/Scientist, Level 4, at $113,00 each) to adequately represent SCE among emergency managers, public health agencies, and other emergency responders in the 13 Counties (Operational Areas) within the 50,000 square mile SCE service territory. Together, this team of professional emergency responders will provide adequate depth of force in the event of extreme regional events that affect large swaths of our customer base.

The new SCE Emergency Managers will be responsible for:

- Establishing and maintaining planning and response relationships with external partners;
- Providing on-scene emergency management expertise for OUs;
- Staffing the Emergency Operation Center (EOC) under normal as well as emergency conditions;
- Validating the content of corporate response plans;
- Partnering with the scientific and natural hazards mitigation community to identify scenarios of concern to SCE and the communities we serve;
- Leading after-action reviews of plan activations or incidents to identify and document improvements and lessons learned; and
- Providing back up to the Mutual Assistance Program Manager.

We also estimate $25,000 for supplies for the EOC, the hub of response coordination between SCE's internal OUs, public emergency agencies, and other responders. The EOC is equipped to permit its use 24/7 during a period in which external sources of supply are unavailable. This means that the EOC must maintain a supply of batteries for radios, plotter paper for situation maps, pens, pencils copier paper, ink cartridges etc. These supplies are also used in the course of exercises performed at the EOC and must be regularly replaced.

Business Resiliency also estimates $18,000 in annual costs for satellite phones so that Emergency Management employees and select critical response and recovery team members are able to communicate from anywhere in the SCE territory.

b) Department Supplies

As a new department with an expanded staff and scope of work, Business Resiliency requires expendable supplies, at an annual cost of $50,000, which will allow us to operate as

an independent organization and support the new staff needed to meet the expanded scope of the new organization.

D. Analysis of Recorded O&M Expenses (Portions of FERC Account 920/921)

Business Resiliency O&M expenses record in FERC Account 920/921. Table III-28 below provides the 2008-2012 recorded adjusted expenses for the Business Resiliency portions of this account.

Table III-28
Business Resiliency
Portions of FERC Account 920-921
2008-2012 Recorded O&M Expenses
(Constant 2012 $000s)

FERC Account 920-921	2008	2009	2010	2011	2012
Labor	728	728	1,264	1,340	1,374
Non-labor	380	341	938	1,114	450
Other	0	0	0	0	0
Total	1,108	1,069	2,202	2,454	1,824

O&M expenses recorded to this account are generally tied to the staffing level necessary to perform the activities within the department. Labor and non-labor expenses remained relatively stable from 2008 to 2009. From 2009 to 2010, labor expenses rose by $536,000, or 74 percent. This change was driven by staffing increases during 2010 to improve SCE-wide business continuity planning. Also during 2010, Business Resiliency retained Ernst and Young (E&Y) to assess the business continuity needs of the company. This work resulted in a non-labor increase of $597,000, or 71 percent, over 2009 levels.

The small labor increase in 2011 over 2010 reflects the full year labor costs for some of the staff hired during 2010. The non-labor increase in 2011 of $176,000, or 19 percent, was driven by outside consulting costs to conduct a Business Impact Analysis (BIA). The BIA was conducted to develop a better understanding of SCE-wide business processes and their criticality. As there were no additional costs for E&Y during 2011, the non-labor increase over 2010 reflects the net increase in costs for the BIA relative to the E&Y work.

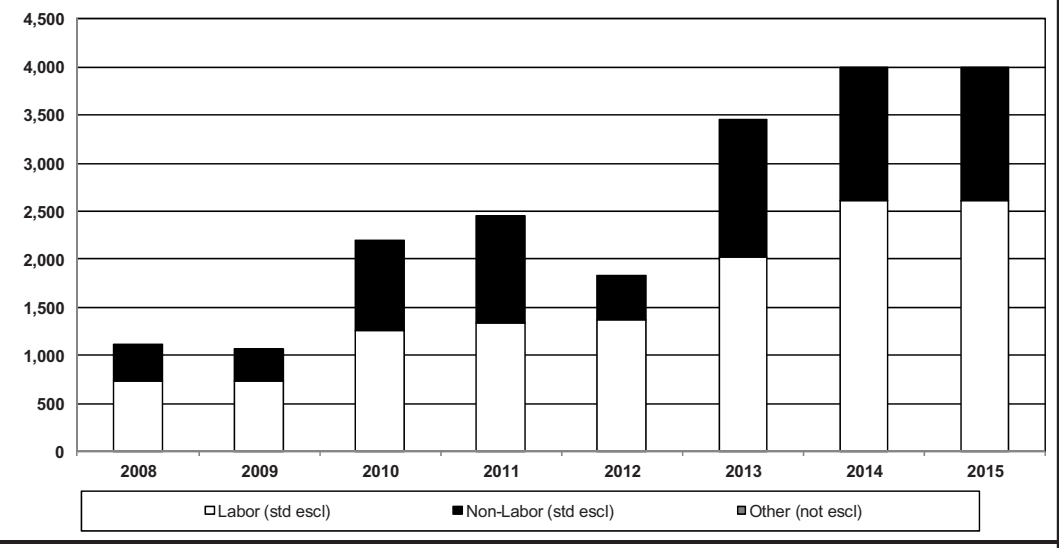
From 2011 to 2012, the staffing level and associated labor expenses remained relatively constant, while non-labor expenses decreased by $664,000, or 60 percent. This drop reflects reduced consulting services expenses in 2012. The 2012 recorded data does reflect a $170,000 adjustment in non-labor expenses to remove the one-time costs of the Davies study conducted in response to the November 2011

windstorm. Labor expenses were also adjusted downward in 2012 by $115,000 to remove costs associated with SCE's response to the 2011 windstorm.

E. Test Year Forecast (portions of FERC Account 920/921)

The 2015 Test Year O&M forecast of $4 million includes a baseline forecast reflecting the ongoing costs of the scope of work performed during the 2012 base year, plus future year adjustments to implement changes to the Business Resiliency organization discussed above. The departments O&M forecast is provided in Figure III-8 below.

Figure III-8
Business Resiliency
Portions of FERC Account 920-921
2013-2015 Forecast O&M Expenses
(Constant 2012 $000s)



	2008	2009	2010	2011	2012	2013	2014	2015
Labor	728	728	1,264	1,340	1,374	2,029	2,609	2,609
Non-Labor	380	341	938	1,114	450	1,434	1,392	1,392
Other	0	0	0	0	0	0	0	0
Total	**1,108**	**1,069**	**2,202**	**2,454**	**1,824**	**3,463**	**4,000**	**4,000**

Forecast

1. 2015 Test Year Base Forecast

SCE is forecasting the costs for ongoing Business Resiliency activities using last recorded year (2012), $1.374 million, for labor expenses and three-year average (2009-2012), $0.834 million, for non-labor expenses.

For labor, last recorded year was selected as the forecast as labor expenses have remained relatively stable over the last three years and the scope of work that this baseline represents is expected to continue through the rate case period 2015-2017. This approach is consistent with D.89-12-057, in which the CPUC stated that for those accounts that have been relatively stable for three or more years, the base year recorded expense is an appropriate base estimate for the Test Year.

For non-labor, SCE is using a three-year averaging technique to forecast costs for ongoing activities performed within the 2012 base year scope of work. The averaging method is appropriate for this account as non-labor expenses have shown significant fluctuations from year to year. Historically, these fluctuations have been driven by costs for outside consulting services, which are difficult to predict. The last three years of recorded data reflect two years (2010 and 2011) with significant BIA-related outside consulting work and one year (2012) with very little outside consulting expenses. This pattern of non-labor expense is representative of the expenses likely to occur during the period 2015-2017 as additional BIAs and other consulting services will be needed. This approach is consistent with D.89-12-057, in which the CPUC stated that for those accounts that have significant fluctuations in recorded expenses from year-to-year, an average of recorded expenses is appropriate to use as a basis for forecasting.

2. Adjustments to 2015 Test Year

To the baseline Test Year forecast discussed above, Business Resiliency forecasts future year adjustments as shown in Table III-29, below.

Table III-29
Business Resiliency
2013-2015 Future Year Adjustments and Total O&M Forecast
(Constant 2012 $000s)

Line #	Adjustment/Forecast	2013	2014	2015
1	Governance	291	463	463
2	Plans and Programs	757	1,020	1,020
3	Emergency Response and Recovery	206	319	319
4	Total Adjustments (Lines 1 + 2 + 3)	1,255	1,792	1,792
5	2015 Base Forecast (see section III.E.1)	2,208	2,208	2,208
6	2015 Total Forecast (Lines 4 + 5)	3,463	4,000	4,000

The table above reflects the phasing-in of staffing during 2013 to implement the new Business Resiliency organization design. The adjustments identified above for the 2015 Test Year reflect full implementation of all incremental costs as described in Section III.C of this testimony.[39]

[39] Please note that the total forecast provided on line 7 may not match the forecast provided in Figure III-8 due to rounding.

Appendix A

Witness Qualifications

SOUTHERN CALIFORNIA EDISON COMPANY

QUALIFICATIONS AND PREPARED TESTIMONY OF

DON DAIGLER

Q. Please state your name and business address for the record.

A. My name is Don Daigler, and my business address is 8631 Rush Street, Room 101, Rosemead, CA 91770.

Q. Briefly describe your present responsibilities at the Southern California Edison Company.

A. I am the Director of Business Resiliency under the Safety, Security, and Compliance (SSC) Organizational Unit (OU). I am responsible for providing governance over the over the Southern California Edison Business Resiliency activities which includes working closely with the company's Enterprise Risk Management program to understand corporate risk and identify ways to minimize their impacts. I also manage the company's emergency management functions for all hazards facing the company's business lines, facilities and people and lead the development and implementation of corporate Business Continuity Plans.

Q. Briefly describe your educational and professional background.

A. I have a BS in Liberal Studies with an educational focus on Health Physics and have more than 30 years of experience in the areas of national security and emergency management. My career includes 26 years of service in the federal government, where I have held several senior leadership positions, both in the field and at the policy level in Washington, D.C. Immediately prior to joining SCE, I was the Response Planning Director for the Federal Emergency Management Agency (FEMA), where I led all national and regional response planning activities and was the planning lead during several large scale disasters, such as hurricanes Sandy, Isaac, and Irene. In that capacity, I was also responsible for leading the agency's chemical, biological, radiological, nuclear, and explosives programs as well as the National Hurricane Program and Remote Sensing Program. Previously, I ran the Technology Integration Program for the Department of Energy's National Nuclear Security Administration, which developed specialized emergency response equipment. Before moving to Washington, D.C., I held leadership roles for

the Department of Energy's Nevada Site Office, including the position of Director of the Homeland Security and Defense Division. My federal government experience also includes experience with the Environmental Protection Agency and the Department of Defense.

Q. What is the purpose of your testimony in this proceeding?

A. The purpose of my testimony in this proceeding is to sponsor Exhibit SCE-07, Volume 4, entitled *Safety, Security & Compliance – Corporate Security and Business Resiliency*.

Q. Was this material prepared by you or under your supervision?

A. Yes, it was with respect to Chapter III (Business Resiliency). With respect to Chapter I (Overview) and Chapter II (Corporate Security), the testimony was originally prepared by, and at the direction of, Jana Monroe. Ms. Monroe was formerly the Director of Corporate Security. I am adopting the testimony contained in Chapters I and II.

Q. Insofar as this material is factual in nature, do you believe it to be correct?

A. Yes, I do.

Q. Insofar as this material is in the nature of opinion or judgment, does it represent your best judgment?

A. Yes, it does.

Q. Does this conclude your qualifications and prepared testimony?

A. Yes, it does.