Risk Assessment and Mitigation Phase
Cross-Functional Factor

(SDG&E-CFF-5)
Physical Security

May 17, 2021

TABLE OF CONTENTS

CROSS-FUNCTIONAL FACTOR: PHYSICAL SECURITY

I. INTRODUCTION

This Physical Security Cross-Functional Factor (CFF) Chapter describes how Physical Security activities impact the risks described in SDG&E's Risk Assessment Mitigation Phase (RAMP) risk Chapters.

SDG&E is presenting CFF information in this RAMP Report to provide the Commission and parties additional information regarding the risks and mitigations described in its RAMP risk chapters. CFFs are not in and of themselves RAMP risks. Rather, CFFs are drivers, triggers, activities or programs that may impact multiple RAMP risks. CFFs are also generally foundational in nature. Therefore, SDG&E's CFF presentation differs from that of its RAMP risk chapters (*e.g.*, no risk spend efficiency calculations or alternatives are provided). SDG&E's CFF chapters provide narrative descriptions of the CFF projects and programs that impact multiple SDG&E's RAMP risk chapters through the 2022-2024 time frame. Related cost forecasts are provided as available, consistent with an expected test year (TY) 2024 general rate case (GRC) request.

As described below, Physical Security is an enterprise-wide framework that provides a standardized approach for managing risk and safety across assets and activities. The Physical Security CFF therefore spans multiple lines of business and helps to mitigate several RAMP risks in this Report.

II. OVERVIEW

Physical security encompasses the systems and activities that maintain the safety of employees, contractors, vendors, the public, SDG&E facilities, and infrastructure, through people, processes, and technology. The three primary categories of physical security are described as follows:

- People – the skill and expertise of employees, contractors, and vendors who implement and support physical security.
- Process – the goals, regulations, guidelines, and instructions that establish actions for risk management (*e.g.*, plans, policies, procedures, training, and awareness).
- Technology – the hardware and software of the physical security system that is designed to deter, delay, detect, assess, communicate, and respond to potential

physical threats (*e.g.*, barriers, closed circuit television (CCTV) system, access management system, video analytics, and electronic keys).

Physical security mitigates incidents such as theft, robbery, burglary, vandalism, sabotage, terrorism and trespassing, which may result in a gas leak, fire, explosion, and/or operational outages. Physical security incidents may have direct safety consequences, such as the potential for serious injury or death related to electrocution, gas leaks or explosions, or may have indirect safety consequences, such as the disruption of electric or gas operations causing downstream outages affecting the general public. Effective physical security is essential to protecting the facilities, assets, and people that provide safe and reliable electric and gas services.

SDG&E implements a layered security system to protect employees, facilities, and infrastructure. Often referred to as "concentric circles of security" or "defense in depth," this principal involves using multiple layers of security to protect high-value assets. At each boundary, there is an opportunity to deter, detect, delay, assess, communicate, or respond to an adversary. This approach improves the opportunity for intruders to be interdicted at each layer with an appropriate security response.

III. ASSOCIATED RISK EVENTS

Physical security is a cross-functional factor affecting several risks including (Incident Related to the Medium Pressure System, Incident Related to the High Pressure System, Excavation Damage (Dig-In) on Gas System, Incident Involving an Employee, Incident Involving a Contractor, Contact with Electric Facilities and Cybersecurity). Physical security is a factor in protecting operational reliability, ensuring the safety of employees and the public, and maintaining compliance with government regulations or guidelines.

IV. 2020 PROJECTS AND PROGRAMS

A. Physical Security Systems

Physical security systems provide protection enhancements to facilities or infrastructure to improve access control, intrusion detection, and interdiction capabilities to deter, detect, delay, assess, communicate, or respond to undesirable events. Examples include, but are not limited to:

- Physical Barriers – Physical barriers are natural and man-made structures that physically and psychologically deter and delay adversaries and channel traffic through specified entry/exit points. Types of barriers include berms, fences, walls, gates, vehicle anti-ramming measures (*e.g.*, bollards, engineered planters

and benches, and landscaping boulders) window barriers, ravines, drainage ditches, and security doors.

- Access Control System – Access control systems limit or detect access to facilities and are commonly integrated across all security layers. They provide separation between common areas and higher security areas or critical assets. Access controls are typically found in the form of the electronic control systems (proximity card readers or electronic keys) and mechanical locks/keys.
- Intrusion Detection System (IDS) – IDS are an array of sensors, surveillance devices, and associated communication systems used to increase the probability of detection and the assessment of potential unauthorized access to facilities. The technologies used in IDS systems range from electrical contact mechanisms, tamper sensors, motion, heat, sound, or vibration sensors, radar, duress alarms, video analytics, and other devices.
- CCTV – CCTV is a self-contained surveillance system comprising cameras, recorders, control equipment, and displays for monitoring activities in real time. The CCTV system is intended to be an overt deterrent used to assess real-time security events and act as a forensic tool for investigations following an incident.

Corporate Security is making physical security planning, implementation, and maintenance more efficient through automation, analysis, and testing. A new access management reporting tool was introduced in 2020 to allow for analysis of access. The reporting tool will assist Corporate Security with identifying information such as locations with high alarm rates and badge access card usage. In addition, a new automated access request process was implemented to streamline the access request and approval process, to allow for performance metrics and analysis, and to reduce labor hours associated with providing access. Finally, a new security equipment testing lab was created to integrate and test the functionality of new security equipment prior to installation.

B. Contract Security

In addition to physical security systems, SDG&E employs contract security (security guards) to secure and protect assets and people. Security personnel are located at critical facilities and other work locations. Security personnel are used to complement and supplement existing security measures. Security personnel can also provide increased security capabilities as

an overt deterrence during security incidents or emergencies. Security personnel may be deployed permanently at a facility based on factors such as criticality, facility population, or compliance; or temporarily based on factors such as the threat environment, criminal activity, and past incidents.

C. Corporate Security Planning, Awareness, Risk Management, and Incident Management

The Corporate Security organization develops planning, awareness, risk management and incident management projects and programs to prevent, mitigate, or respond to security incidents. This control includes Corporate Security labor (training, investigations, etc.), intelligence services, and the Case Management System, which is used to track security incidents and investigations. This control incorporates services provided by Corporate Security, including:

- Physical security operations responsible for planning, design, development, testing, implementation, maintenance, integration, and coordination of physical security systems.
- Risk management to identify, assess, control, and monitor physical security risks potentially impacting the company.
- Intelligence analysis to continually assess threats and develop actionable intelligence for risk mitigation, security planning, infrastructure protection, and employee safety.
- Investigation of security incidents to determine and assist with corrective actions, litigation, and security practice improvement.
- Training, exercises, and drills of employees and public safety agencies to improve security awareness and response.
- Incident management to respond to incidents and coordinate with public safety agencies or other appropriate parties.
- Security oversight to establish and enforce regulations, guidelines, plans, policies, and procedures.

V. 2022-2024 PROJECTS AND PROGRAMS

Planning, Awareness, Risk Management, and Incident Management activities are tracked through a variety of methods. Physical security operations incorporate bi-weekly meetings to plan, design, develop, test, implement, maintain and coordinate physical security systems. Risk

management occurs at various levels including annual risk assessments, ongoing threat evaluations, and regulatory vulnerability assessments. Security incidents and investigations are tracked within a case management database. Analysis and review of security incidents are performed on a monthly and on an ad hoc basis by the director and managers of Corporate Security. Security guidelines, plans, policies, and procedures are reviewed regularly to complete appropriate updates.

A. Physical Security Upgrades

SDG&E plans to expand physical security upgrades to replace end of life equipment, to improve integration, to reduce nuisance alarms, and to incorporate recent industry security technology enhancements. Security enhancements to facilities and infrastructure improve access control, intrusion detection, and interdiction capabilities to deter, detect, delay, communicate, and respond to undesirable events.

B. Corporate Security Agent

SDG&E plans to expand its workforce to support Corporate Security. Expansion of the workforce will provide additional coverage of the large service area, reduce response time to security incidents, and increase the number of Site Security Reviews. This will determine security threats and mitigate vulnerabilities to ensure the safety of employees and the public, secure infrastructure and improve electric system and gas reliability.

VI. COSTS

Table 1 contains the 2020 recorded and forecast dollars for the programs and projects discussed in this CFF.

Table 1: Costs (Direct After Allocations, in 2020 $000)[1]

Line No.	Description	Recorded		Forecast			
		2020 Capital	2020 O&M	2022-2024 Capital (Low)	2022-2024 Capital (High)	TY 2024 O&M (Low)	TY 2024 O&M (High)
1	Physical Security	1,133	0	3,653	4,465	0	0
2	Contract Security	115	2,330	673	823	2,320	2,836
3	Planning, Awareness, Risk Management, and Incident Management	0	568	0	0	528	607
4	Physical Security Upgrades	Included in line 1	0	Included in line 1	Included in line 1	0	0
5	Corporate Security Agent	Included in line 2	0	Included in line 2	Included in line 2	0	0

[1] Costs presented in the workpapers may differ from this table due to rounding. The figures provided are direct charges and do not include company loaders, with the exception of vacation and sick. The costs are also in 2020 dollars and have not been escalated in forecasts beyond 2020.