

Application of SOUTHERN CALIFORNIA GAS)
COMPANY for authority to update its gas revenue)
requirement and base rates)
effective January 1, 2019 (U 904-G))

Application No. 17-10-____
Exhibit No.: (SCG-27-CWP)

CAPITAL WORKPAPERS TO
PREPARED DIRECT TESTIMONY
OF GAVIN H. WORDEN
ON BEHALF OF SOUTHERN CALIFORNIA GAS COMPANY

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

OCTOBER 2017



2019 General Rate Case - APP
INDEX OF WORKPAPERS

Exhibit SCG-27-CWP - CYBER SECURITY

DOCUMENT	PAGE
Overall Summary For Exhibit No. SCG-27-CWP	1
Category: A. PROTECT	2
..00758A - RAMP - INCREMENTAL PKI REBUILD	5
..00758B - RAMP - INCREMENTAL FIREWALL SECURITY	11
..00758G - RAMP - INCREMENTAL FOF - CONVERGED PERIMETER SECURITY	17
..00758H - RAMP - INCREMENTAL FOF - HOST BASED PROTECTION	23
..00758J - RAMP - INCREMENTAL EMAIL SPAM PROTECTION	31
..00758K - RAMP - INCREMENTAL IS ZONE REBUILD	39
..00758M - RAMP - INCREMENTAL SECURITY ORCHESTRATION	45
..00758N - RAMP - INCREMENTAL CRITICAL GAS INFRASTRUCTURE PROTECTION	53
..00758O - RAMP - INCREMENTAL CRITICAL GAS INFRASTRUCTURE PROTECTION - 2018	61
..00758P - RAMP - INCREMENTAL CRITICAL GAS INFRASTRUCTURE PROTECTION - 2019	69
..00758Q - RAMP - INCREMENTAL CASB (CLOUD DATA USE)	77
..00758R - RAMP - INCREMENTAL WEB APPLICATIONS AND DATABASE FIREWALLS	85
..00758U - RAMP - INCREMENTAL ENTERPRISE SOURCE CODE SECURITY	91
..00758V - RAMP - INCREMENTAL WIRED NETWORK PREVENTATIVE CONTROLS	99
..00758W - RAMP - INCREMENTAL MULTI FACTOR AUTHENTICATION REFRESH	105
..00758X - RAMP - INCREMENTAL MY ACCOUNT MULTI FACTOR AUTHENTICATION	113
Category: B. DETECT	119
..00758AA - RAMP - INCREMENTAL THREAT RESPONSE SYSTEMS	121
..00758AB - RAMP - INCREMENTAL THREAT RECOVERY SYSTEMS	129
..00758D - RAMP - INCREMENTAL SCG NETWORK ANOMALY DETECTION PHASE 1	137
..00758F - RAMP - INCREMENTAL INSIDER THREAT DETECTION / PREVENTION	145
..00758I - RAMP - INCREMENTAL SSL DECRYPTION	153
..00758L - RAMP - INCREMENTAL NETWORK SECURITY MONITORING	159
..00758S - RAMP - INCREMENTAL PERIMETER TAP INFRASTRUCTURE REDESIGN	167
..00758Z - RAMP - INCREMENTAL THREAT DETECTION SYSTEMS	173
Category: C. RESPOND	185
..00758C - RAMP - INCREMENTAL FORENSICS SYSTEM REBUILD	186
..00758T - RAMP - INCREMENTAL INCIDENT RESPONSE SECURE COLLABORATION	192
Category: D. IDENTIFY	200
..00758E - RAMP - INCREMENTAL ENTERPRISE THREAT INTELLIGENCE	201
..00758Y - RAMP - INCREMENTAL THREAT IDENTIFICATION SYSTEMS	209

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Overall Summary For Exhibit No. SCG-27-CWP

Area:	CYBER SECURITY
Witness:	Gavin H. Worden

In 2016 \$ (000)			
Adjusted-Forecast			
	2017	2018	2019
A. PROTECT	10,515	16,085	4,807
B. DETECT	5,653	1,477	13,193
C. RESPOND	202	1,914	0
D. IDENTIFY	1,474	0	4,731
Total	17,844	19,476	22,731

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Category: A. PROTECT
Workpaper: VARIOUS

Summary for Category: A. PROTECT

	In 2016\$ (000)			
	Adjusted-Recorded	Adjusted-Forecast		
	2016	2017	2018	2019
Labor	0	813	1,035	398
Non-Labor	0	8,868	15,050	4,409
NSE	0	834	0	0
Total	0	10,515	16,085	4,807
FTE	0.0	6.5	9.0	3.6

00758A RAMP - Incremental PKI Rebuild

Labor	0	58	0	0
Non-Labor	0	0	0	0
NSE	0	0	0	0
Total	0	58	0	0
FTE	0.0	0.5	0.0	0.0

00758B RAMP - Incremental Firewall Security

Labor	0	58	0	0
Non-Labor	0	250	0	0
NSE	0	0	0	0
Total	0	308	0	0
FTE	0.0	0.5	0.0	0.0

00758G RAMP - Incremental FOF - Converged Perimeter Security

Labor	0	116	70	0
Non-Labor	0	2,400	1,200	0
NSE	0	0	0	0
Total	0	2,516	1,270	0
FTE	0.0	1.0	0.7	0.0

00758H RAMP - Incremental FOF - Host Based Protection

Labor	0	116	23	0
Non-Labor	0	2,151	0	0
NSE	0	0	0	0
Total	0	2,267	23	0
FTE	0.0	1.0	0.2	0.0

00758J RAMP - Incremental Email Spam Protection

Labor	0	105	0	0
Non-Labor	0	147	0	0
NSE	0	834	0	0
Total	0	1,086	0	0
FTE	0.0	1.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Category: A. PROTECT
Workpaper: VARIOUS

	In 2016\$ (000)			
	Adjusted-Recorded	Adjusted-Forecast		
	2016	2017	2018	2019
00758K RAMP - Incremental IS Zone Rebuild				
Labor	0	81	0	0
Non-Labor	0	820	0	0
NSE	0	0	0	0
Total	0	901	0	0
FTE	0.0	0.5	0.0	0.0
00758M RAMP - Incremental Security Orchestration				
Labor	0	105	35	0
Non-Labor	0	1,600	150	0
NSE	0	0	0	0
Total	0	1,705	185	0
FTE	0.0	1.0	0.5	0.0
00758N RAMP - Incremental Critical Gas Infrastructure Protection				
Labor	0	174	0	0
Non-Labor	0	1,500	0	0
NSE	0	0	0	0
Total	0	1,674	0	0
FTE	0.0	1.0	0.0	0.0
00758O RAMP - Incremental Critical Gas Infrastructure Protection - 2018				
Labor	0	0	291	0
Non-Labor	0	0	2,000	0
NSE	0	0	0	0
Total	0	0	2,291	0
FTE	0.0	0.0	2.5	0.0
00758P RAMP - Incremental Critical Gas Infrastructure Protection - 2019				
Labor	0	0	0	232
Non-Labor	0	0	0	4,000
NSE	0	0	0	0
Total	0	0	0	4,232
FTE	0.0	0.0	0.0	2.0
00758Q RAMP - Incremental CASB (cloud data use)				
Labor	0	0	93	0
Non-Labor	0	0	2,800	0
NSE	0	0	0	0
Total	0	0	2,893	0
FTE	0.0	0.0	1.0	0.0
00758R RAMP - Incremental Web Applications and Database Firewalls				
Labor	0	0	128	0
Non-Labor	0	0	2,100	0
NSE	0	0	0	0
Total	0	0	2,228	0
FTE	0.0	0.0	1.1	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Category: A. PROTECT
Workpaper: VARIOUS

	In 2016\$ (000)			
	Adjusted-Recorded	Adjusted-Forecast		
	2016	2017	2018	2019
00758U RAMP - Incremental Enterprise Source Code Security				
Labor	0	0	80	36
Non-Labor	0	0	1,100	0
NSE	0	0	0	0
Total	0	0	1,180	36
FTE	0.0	0.0	0.8	0.4
00758V RAMP - Incremental Wired Network Preventative Controls				
Labor	0	0	175	60
Non-Labor	0	0	3,200	0
NSE	0	0	0	0
Total	0	0	3,375	60
FTE	0.0	0.0	1.0	0.6
00758W RAMP - Incremental Multi Factor Authentication Refresh				
Labor	0	0	140	0
Non-Labor	0	0	2,500	0
NSE	0	0	0	0
Total	0	0	2,640	0
FTE	0.0	0.0	1.2	0.0
00758X RAMP - Incremental My Account Multi Factor Authentication				
Labor	0	0	0	70
Non-Labor	0	0	0	409
NSE	0	0	0	0
Total	0	0	0	479
FTE	0.0	0.0	0.0	0.6

Note: Totals may include rounding differences.

Beginning of Workpaper Group
00758A - RAMP - Incremental PKI Rebuild

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758A - RAMP - Incremental PKI Rebuild

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	58	0	0
Non-Labor	Zero-Based	0	0	0	0	0	0	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	58	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0

Business Purpose:

Our enterprise PKI currently uses the SHA-1 signature algorithm. SHA-1 algorithm has been widely used since 1985 but is vulnerable to hacking and is no longer recommended for PKI. Microsoft, Google and other major providers will not recognize certificates signed using SHA-1 after January 1, 2017. The impact to our users (and potentially customers) will be a series of escalating trust notifications beginning December 2015 and eventual loss of access to systems.

Physical Description:

To secure our websites, intranet communications and applications we must build a new PKI infrastructure using SHA-2 in parallel to the current SHA-1 PKI and issue new certificates to all dependent systems.

Project Justification:

Enhance security of company websites, intranet communications and applications. Certificate Authorities servers will enable consolidation of systems, simplify support and reduce support complexity. Upgrade to MS Server 2012 will improve high-volume certificate issuance and certificate enrollment across Active Directory Domain Services forest boundaries.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758A - RAMP - Incremental PKI Rebuild

Forecast Methodology:

Labor - Zero-Based

Project is currently in-flight. Based on actual timeline of the project to complete.

Non-Labor - Zero-Based

Project is currently in-flight. Based on actual timeline of the project to complete.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758A**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758A - RAMP - Incremental PKI Rebuild
 Workpaper Detail: 00758A.001 - RAMP - Incremental PKI Rebuild
 In-Service Date: 01/31/2017

Description:

Self developed software

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		58	0	0
Non-Labor		0	0	0
NSE		0	0	0
	Total	58	0	0
FTE		0.5	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758A - RAMP - Incremental PKI Rebuild
 Workpaper Detail: 00758A.001 - RAMP - Incremental PKI Rebuild

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Public Key Infrastructure

Program Description: PKI digital key encryption system to protect in transit and to authenticate devices, services, and applications

Deploy SHA2 compliance public key infrastructure for digital certificates

Risk/Mitigation:

Risk: All Cyber Security Risks

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758B - RAMP - Incremental Firewall Security

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758B - RAMP - Incremental Firewall Security

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	58	0	0
Non-Labor	Zero-Based	0	0	0	0	0	250	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	308	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0

Business Purpose:

The Cybersecurity Protect function refers to developing and implementing the appropriate safeguards so that the company can provide safe and reliable delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of control Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Protection-oriented activities are focused on avoiding or limiting potential cybersecurity events. Activities in this functional area include: managing asset access, cybersecurity awareness and training, protective technologies, and system maintenance. Ongoing cybersecurity awareness and training is important for engaging all employees so that they understand their roles and responsibilities regarding cybersecurity. Other activities in this area include vulnerability management, system implementation, security consulting and support, and operating support for protection systems. This support can include: two-factor authentication, the public key infrastructure, malware prevention, web content management, and supporting network protections, such as firewalls and intrusion detection and prevention.

Physical Description:

Evaluate and deploy a firewall management system (hardware and software) to control outbound firewall egress policies, Prevent unauthorized access to firewall, centrally managed configurations , mitigate vulnerabilities using industry standard best practices, Secure the Enterprise network perimeter and internal firewalls.

Project Justification:

Reduced risk of business system outages, data loss, and malware proliferation. Increased efficiency in firewall request approval and risk assessment and enhancing current capabilities.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758B - RAMP - Incremental Firewall Security

Forecast Methodology:

Labor - Zero-Based

Project is currently in-flight. Based on actual timeline of the project to complete.

Non-Labor - Zero-Based

Project is currently in-flight. Based on actual timeline of the project to complete.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758B**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758B - RAMP - Incremental Firewall Security
 Workpaper Detail: 00758B.001 - RAMP - Incremental Firewall Security
 In-Service Date: 02/28/2017

Description:

Tufin upgrade

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		58	0	0
Non-Labor		250	0	0
NSE		0	0	0
	Total	308	0	0
FTE		0.5	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758B - RAMP - Incremental Firewall Security
 Workpaper Detail: 00758B.001 - RAMP - Incremental Firewall Security

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Web Applications and Database Firewalls

Program Description: Firewall Security

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Construction Start Date:

In Service Date:02/28/2017

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758G - RAMP - Incremental FOF - Converged Perimeter Security

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758G - RAMP - Incremental FOF - Converged Perimeter Security

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	116	70	0
Non-Labor	Zero-Based	0	0	0	0	0	2,400	1,200	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	2,516	1,270	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.0	0.7	0.0

Business Purpose:

Simplify network perimeter cybersecurity systems to improve ability to monitor and support protection and detection functions.

Physical Description:

The scope of this project will focus on firewalls (4) and Intrusion Prevention Devices (6) at the data center perimeters. Project team will be formed to develop and RFP to identify viable alternatives and conduct on site evaluations to determine the best solution.

Project Justification:

Enhance cybersecurity controls of perimeter and provide operational efficiencies.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758G - RAMP - Incremental FOF - Converged Perimeter Security

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758G**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758G - RAMP - Incremental FOF - Converged Perimeter Security
 Workpaper Detail: 00758G.001 - RAMP - Incremental Fueling Our Future 760
 In-Service Date: 06/30/2018
 Description:

FOF IDEA # 760

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		116	70	0
Non-Labor		2,400	1,200	0
NSE		0	0	0
	Total	2,516	1,270	0
FTE		1.0	0.7	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758G - RAMP - Incremental FOF - Converged Perimeter Security
 Workpaper Detail: 00758G.001 - RAMP - Incremental Fueling Our Future 760

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Converged Perimeter Systems

Program Description: Converged Perimeter Systems - FOF 760

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758H - RAMP - Incremental FOF - Host Based Protection

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758H - RAMP - Incremental FOF - Host Based Protection

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	116	23	0
Non-Labor	Zero-Based	0	0	0	0	0	2,151	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	2,267	23	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.0	0.2	0.0

Business Purpose:

Continued implementation of separate systems causes additional infrastructure need, multi-vendor incompatibility and additional endpoint agents that compete for system resources.

Physical Description:

Servers would be included in the scope of this project.

Project Justification:

Virtualized servers will be better protected and resilient when located outside the protected perimeter, such as being placed in cloud environments or connecting to the network while working offsite.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758H - RAMP - Incremental FOF - Host Based Protection

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758H**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758H - RAMP - Incremental FOF - Host Based Protection
 Workpaper Detail: 00758H.001 - RAMP - Incremental Fueling Our Future 790
 In-Service Date: 03/31/2018

Description:

Self developed software portion of the project. FOF IDEA # 790
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		116	23	0
Non-Labor		324	0	0
NSE		0	0	0
	Total	440	23	0
FTE		1.0	0.2	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758H - RAMP - Incremental FOF - Host Based Protection
 Workpaper Detail: 00758H.001 - RAMP - Incremental Fueling Our Future 790

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Host Based Protection

Program Description: Host Based Protection - FOF 790

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758H - RAMP - Incremental FOF - Host Based Protection
 Workpaper Detail: 00758H.002 - RAMP - Incremental Fueling Our Future 790
 In-Service Date: 03/31/2018

Description:

License/materials purchase (non self developed)

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	0
Non-Labor		1,827	0	0
NSE		0	0	0
	Total	<u>1,827</u>	<u>0</u>	<u>0</u>
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758H - RAMP - Incremental FOF - Host Based Protection
 Workpaper Detail: 00758H.002 - RAMP - Incremental Fueling Our Future 790

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Hosted Based Protection

Program Description: Hosted Based Protection - FOF 790

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758J - RAMP - Incremental Email Spam Protection

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758J - RAMP - Incremental Email Spam Protection

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	105	0	0
Non-Labor	Zero-Based	0	0	0	0	0	147	0	0
NSE	Zero-Based	0	0	0	0	0	834	0	0
Total		0	0	0	0	0	1,086	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0

Business Purpose:

The Cybersecurity Protect function refers to developing and implementing the appropriate safeguards so that the company can provide safe and reliable delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of control Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Protection-oriented activities are focused on avoiding or limiting potential cybersecurity events. Activities in this functional area include: managing asset access, cybersecurity awareness and training, protective technologies, and system maintenance. Ongoing cybersecurity awareness and training is important for engaging all employees so that they understand their roles and responsibilities regarding cybersecurity. Other activities in this area include vulnerability management, system implementation, security consulting and support, and operating support for protection systems. This support can include: two-factor authentication, the public key infrastructure, malware prevention, web content management and supporting network protections such as firewalls and intrusion detection and prevention.

Physical Description:

Deployment of email protection system hardware and software.

Project Justification:

The legacy email provides spam filter and malware defense system for all internal and external email that has reached end of life. Select and deploy a current state system.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758J - RAMP - Incremental Email Spam Protection

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758J**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758J - RAMP - Incremental Email Spam Protection
 Workpaper Detail: 00758J.001 - RAMP - Incremental RFP to evaluate and upgrade spam malware filter
 In-Service Date: 10/31/2017

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		105	0	0
Non-Labor		147	0	0
NSE		0	0	0
	Total	252	0	0
FTE		1.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758J - RAMP - Incremental Email Spam Protection
 Workpaper Detail: 00758J.001 - RAMP - Incremental RFP to evaluate and upgrade spam malware filter

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Email and Web Browser Protections

Program Description: Solution deployment for internet email spam, phishing and malware filtering

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758J - RAMP - Incremental Email Spam Protection
 Workpaper Detail: 00758J.002 - RAMP - Incremental RFP to evaluate and upgrade spam malware filter - SDS
 In-Service Date: 10/31/2017

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		0	0	0
NSE		834	0	0
	Total	834	0	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758J - RAMP - Incremental Email Spam Protection
 Workpaper Detail: 00758J.002 - RAMP - Incremental RFP to evaluate and upgrade spam malware filter - SDS

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Email and Web Browser Protections

Program Description: Solution deployment for internet email spam, phishing and malware filtering

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758K - RAMP - Incremental IS Zone Rebuild

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758K - RAMP - Incremental IS Zone Rebuild

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	81	0	0
Non-Labor	Zero-Based	0	0	0	0	0	820	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	901	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0

Business Purpose:

Ensure continued network reliability and ensure recovery is quick and supported in the event of a hardware or software network device failure.

Physical Description:

Replace all network switches in both RB and MPK IS physical zones and upgrade the connectivity between racks to 10GB. Replace KVMS equipment.

Project Justification:

Timely replacement of technology infrastructure

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758K - RAMP - Incremental IS Zone Rebuild

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758K**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758K - RAMP - Incremental IS Zone Rebuild
 Workpaper Detail: 00758K.001 - RAMP - Incremental replace switches and IPS IS zone
 In-Service Date: 11/30/2017

Description:

replace switches and IPS IS zone

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		81	0	0
Non-Labor		820	0	0
NSE		0	0	0
	Total	901	0	0
FTE		0.5	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758K - RAMP - Incremental IS Zone Rebuild
 Workpaper Detail: 00758K.001 - RAMP - Incremental replace switches and IPS IS zone

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: IS Zone Rebuild

Program Description: Replace switches and IPS in IS zone

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758M - RAMP - Incremental Security Orchestration

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758M - RAMP - Incremental Security Orchestration

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	105	35	0
Non-Labor	Zero-Based	0	0	0	0	0	1,600	150	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	1,705	185	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.0	0.5	0.0

Business Purpose:

The Cybersecurity Respond function refers to developing and implementing the appropriate activities to take action regarding a detected Cybersecurity event. The Respond Function supports the ability to contain the impact of a potential Cybersecurity event. Examples of control Categories within this Function include: Response Planning; Communications; Analysis; Mitigation and Improvements.

The Incident Response team coordinates cybersecurity incident response activities when a security event is escalated. They also provide analysis of the incident, during the incident, to determine the most effective response, as well as after the incident in terms of lessons learned. During the incident, communications with stakeholders are maintained. This functional area is the focus of ongoing training to maintain readiness through exercises to validate the response plans for high impact systems.

Physical Description:

Automation of repeatable Information Security Operations Center tasks on the business network.

Project Justification:

Currently many repeatable incident reponse processes are handled manually. These repeatable incident response tasks could be executed more effectively and more quickly through process automation, freeing up analyst time to focus on higher value tasks.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758M - RAMP - Incremental Security Orchestration

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758M**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758M - RAMP - Incremental Security Orchestration
 Workpaper Detail: 00758M.001 - RAMP - Incremental Automate key security triage tasks
 In-Service Date: 03/31/2018

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		105	35	0
Non-Labor		240	150	0
NSE		0	0	0
	Total	345	185	0
FTE		1.0	0.5	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758M - RAMP - Incremental Security Orchestration
 Workpaper Detail: 00758M.001 - RAMP - Incremental Automate key security triage tasks

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Security Orchestration

Program Description: Automate key security triage tasks

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Respond

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758M - RAMP - Incremental Security Orchestration
 Workpaper Detail: 00758M.002 - RAMP - Incremental Automate key security triage tasks
 In-Service Date: 03/31/2018

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	0
Non-Labor		1,360	0	0
NSE		0	0	0
	Total	1,360	0	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758M - RAMP - Incremental Security Orchestration
 Workpaper Detail: 00758M.002 - RAMP - Incremental Automate key security triage tasks

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Security Orchestration

Program Description: Automate key security triage tasks

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Respond

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758N - RAMP - Incremental Critical Gas Infrastructure Protection

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758N - RAMP - Incremental Critical Gas Infrastructure Protection

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	174	0	0
Non-Labor	Zero-Based	0	0	0	0	0	1,500	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	1,674	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0

Business Purpose:

The Cybersecurity Protect function refers to developing and implementing the appropriate safeguards so that the company can provide safe and reliable delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of control Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Protection-oriented activities are focused on avoiding or limiting potential cybersecurity events. Activities in this functional area include: managing asset access, cybersecurity awareness and training, protective technologies, and system maintenance. Ongoing cybersecurity awareness and training is important for engaging all employees so that they understand their roles and responsibilities regarding cybersecurity. Other activities in this area include vulnerability management, system implementation, security consulting and support, and operating support for protection systems. This support can include: two-factor authentication, the public key infrastructure, malware prevention, web content management, and supporting network protections, such as firewalls and intrusion detection and prevention.

Physical Description:

Evaluate and deploy hardware and software meet cybersecurity protection requirements

Project Justification:

- Cost estimated are based on cybersecurity subject matter experts and historical experience responding to changing priorities and risks to address:
- Timely implementation of technology controls
- Addressing evolving threat capabilities
- Supporting and/or leveraging new technologies

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758N - RAMP - Incremental Critical Gas Infrastructure Protection

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758N**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758N - RAMP - Incremental Critical Gas Infrastructure Protection
 Workpaper Detail: 00758N.001 - RAMP - Incremental Gas infrastructure protection systems - 2017
 In-Service Date: 11/30/2017

Description:

Self developed software portion of the project

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		174	0	0
Non-Labor		225	0	0
NSE		0	0	0
	Total	399	0	0
FTE		1.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758N - RAMP - Incremental Critical Gas Infrastructure Protection
 Workpaper Detail: 00758N.001 - RAMP - Incremental Gas infrastructure protection systems - 2017

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Critical Gas Infrastructure Protection

Program Description: Critical Gas Infrastructure Protection

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Work Paper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758N - RAMP - Incremental Critical Gas Infrastructure Protection
 Workpaper Detail: 00758N.002 - RAMP - Incremental Gas infrastructure protection - 2017
 In-Service Date: 11/30/2017

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	0
Non-Labor		1,275	0	0
NSE		0	0	0
	Total	<u>1,275</u>	<u>0</u>	<u>0</u>
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758N - RAMP - Incremental Critical Gas Infrastructure Protection
 Workpaper Detail: 00758N.002 - RAMP - Incremental Gas infrastructure protection - 2017

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Critical Gas Infrastructure Protection

Program Description: Critical Gas Infrastructure Protection

Risk/Mitigation:

Risk: A major cyber security incident that causes disruption

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Work Paper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
007580 - RAMP - Incremental Critical Gas Infrastructure Protection - 2018

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758O - RAMP - Incremental Critical Gas Infrastructure Protection - 2018

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	291	0
Non-Labor	Zero-Based	0	0	0	0	0	0	2,000	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	2,291	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	2.5	0.0

Business Purpose:

The Cybersecurity Protect function refers to developing and implementing the appropriate safeguards so that the company can provide safe and reliable delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of control Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Protection-oriented activities are focused on avoiding or limiting potential cybersecurity events. Activities in this functional area include: managing asset access, cybersecurity awareness and training, protective technologies, and system maintenance. Ongoing cybersecurity awareness and training is important for engaging all employees so that they understand their roles and responsibilities regarding cybersecurity. Other activities in this area include vulnerability management, system implementation, security consulting and support, and operating support for protection systems. This support can include: two-factor authentication, the public key infrastructure, malware prevention, web content management, and supporting network protections, such as firewalls and intrusion detection and prevention.

Physical Description:

Evaluate and deploy hardware and software meet cybersecurity protection requirements.

Project Justification:

- Cost estimated are based on cybersecurity subject matter experts and historical experience responding to changing priorities and risks to address:
- Timely implementation of technology controls
- Addressing evolving threat capabilities
- Supporting and/or leveraging new technologies

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758O - RAMP - Incremental Critical Gas Infrastructure Protection - 2018

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 007580**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758O - RAMP - Incremental Critical Gas Infrastructure Protection - 2018
 Workpaper Detail: 00758O.001 - RAMP - Incremental Gas infrastructure protection
 In-Service Date: 10/31/2018

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	291	0
Non-Labor		0	300	0
NSE		0	0	0
	Total	0	591	0
FTE		0.0	2.5	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758O - RAMP - Incremental Critical Gas Infrastructure Protection - 2018
 Workpaper Detail: 00758O.001 - RAMP - Incremental Gas infrastructure protection

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Critical Gas Infrastructure Protection - 2018

Program Description: Critical Gas Infrastructure Protection - 2018

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758O - RAMP - Incremental Critical Gas Infrastructure Protection - 2018
 Workpaper Detail: 00758O.002 - RAMP - Incremental Gas infrastructure protection
 In-Service Date: 10/31/2018

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	0
Non-Labor		0	1,700	0
NSE		0	0	0
	Total	<u>0</u>	<u>1,700</u>	<u>0</u>
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758O - RAMP - Incremental Critical Gas Infrastructure Protection - 2018
 Workpaper Detail: 00758O.002 - RAMP - Incremental Gas infrastructure protection

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Critical Gas Infrastructure Protection - 2018

Program Description: Critical Gas Infrastructure Protection - 2018

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758P - RAMP - Incremental Critical Gas Infrastructure Protection - 2019

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758P - RAMP - Incremental Critical Gas Infrastructure Protection - 2019

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	232	
Non-Labor	Zero-Based	0	0	0	0	0	0	4,000	
NSE	Zero-Based	0	0	0	0	0	0	0	
Total		0	0	0	0	0	0	4,232	
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	2.0	

Business Purpose:

The Cybersecurity Protect function refers to developing and implementing the appropriate safeguards so that the company can provide safe and reliable delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of control Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance and Protective Technology.

Protection-oriented activities are focused on avoiding or limiting potential cybersecurity events. Activities in this functional area include: managing asset access, cybersecurity awareness and training, protective technologies, and system maintenance. Ongoing cybersecurity awareness and training is important for engaging all employees so that they understand their roles and responsibilities regarding cybersecurity. Other activities in this area include vulnerability management, system implementation, security consulting and support, and operating support for protection systems. This support can include: two-factor authentication, the public key infrastructure, malware prevention, web content management, and supporting network protections, such as firewalls and intrusion detection and prevention.

Physical Description:

Evaluate and deploy hardware and software meet cybersecurity protection requirements.

Project Justification:

- Cost estimated are based on cybersecurity subject matter experts and historical experience responding to changing priorities and risks to address:
- Timely implementation of technology controls
- Addressing evolving threat capabilities
- Supporting and/or leveraging new technologies

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758P - RAMP - Incremental Critical Gas Infrastructure Protection - 2019

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758P**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758P - RAMP - Incremental Critical Gas Infrastructure Protection - 2019
 Workpaper Detail: 00758P.001 - RAMP - Incremental Gas infrastructure protection
 In-Service Date: 10/31/2019

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	232
Non-Labor		0	0	600
NSE		0	0	0
	Total	0	0	832
FTE		0.0	0.0	2.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758P - RAMP - Incremental Critical Gas Infrastructure Protection - 2019
 Workpaper Detail: 00758P.001 - RAMP - Incremental Gas infrastructure protection

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Critical Gas Infrastructure Protection

Program Description: Critical Gas Infrastructure Protection - 2019

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758P - RAMP - Incremental Critical Gas Infrastructure Protection - 2019
 Workpaper Detail: 00758P.002 - RAMP - Incremental Gas infrastructure protection
 In-Service Date: 10/31/2019

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	0
Non-Labor		0	0	3,400
NSE		0	0	0
	Total	0	0	3,400
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758P - RAMP - Incremental Critical Gas Infrastructure Protection - 2019
 Workpaper Detail: 00758P.002 - RAMP - Incremental Gas infrastructure protection

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Critical Gas Infrastructure Protection

Program Description: Critical Gas Infrastructure Protection - 2019

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpapers

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758Q - RAMP - Incremental CASB (cloud data use)

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758Q - RAMP - Incremental CASB (cloud data use)

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	93	0
Non-Labor	Zero-Based	0	0	0	0	0	0	2,800	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	2,893	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0

Business Purpose:

Implement the ability to monitor services, policy enforcement and data loss in cloud solution.

Physical Description:

Deploy CASB appliances at the data centers and acquire software licensing from top tier provider in time to support enterprise deployment of cloud technologies.

Project Justification:

- Greater ability to identify, react, respond, and recover from a sensitive information extraction and cyber security incident
- Limit potential impact due to a cyber security incident
- Ability to leverage this technology for future requirements

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758Q - RAMP - Incremental CASB (cloud data use)

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758Q**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758Q - RAMP - Incremental CASB (cloud data use)
 Workpaper Detail: 00758Q.001 - RAMP - Incremental Cloud Access Security Broker i.e. Netskope RSA
 In-Service Date: 08/31/2018

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	93	0
Non-Labor		0	420	0
NSE		0	0	0
	Total	0	513	0
FTE		0.0	1.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758Q - RAMP - Incremental CASB (cloud data use)
 Workpaper Detail: 00758Q.001 - RAMP - Incremental Cloud Access Security Broker i.e. Netskope RSA

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: CASB (cloud data use)

Program Description: CASB (cloud data use)

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758Q - RAMP - Incremental CASB (cloud data use)
 Workpaper Detail: 00758Q.002 - RAMP - Incremental Cloud Access Security Broker i.e. Netskope RSA
 In-Service Date: 08/31/2018

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		0	2,380	0
NSE		0	0	0
	Total	0	2,380	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758Q - RAMP - Incremental CASB (cloud data use)
 Workpaper Detail: 00758Q.002 - RAMP - Incremental Cloud Access Security Broker i.e. Netskope RSA

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: CASB (cloud data use)

Program Description: CASB (cloud data use)

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758R - RAMP - Incremental Web Applications and Database Firewalls

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758R - RAMP - Incremental Web Applications and Database Firewalls

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	128	0
Non-Labor	Zero-Based	0	0	0	0	0	0	2,100	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	2,228	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	1.1	0.0

Business Purpose:

WAF implementation would defend and alert against attacks that have been the most common vectors of attack. It would also allow us to protect systems in production with undiscovered (zero day) vulnerabilities. This capability would provide a development team more time to fix issues while not impeding deployment schedules.

Physical Description:

This project will implement a High Availability WAF configuration located at both datacenters to protect web facing systems, and enhance response to vulnerabilities as well as the system's availability SLAs. The WAF placement would initially protect web facing servers that handle sensitive data or that connect to systems that contain sensitive data. Other systems would then be added as capacity allows. This system would integrate with current cybersecurity systems for Web Services protection.

Project Justification:

Provides an extra layer of protection for web applications and databases by implementing a general protection versus mis-use as well as a method to quickly address an incident or vulnerability without modifying the underlying application. The quick response capability is particularly valuable in situations where a new vulnerability has been discovered but no patch has been made available.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758R - RAMP - Incremental Web Applications and Database Firewalls

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758R**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758R - RAMP - Incremental Web Applications and Database Firewalls
 Workpaper Detail: 00758R.001 - RAMP - Incremental Security controls on servers. Deploy web application firewalls
 In-Service Date: 09/30/2018

Description:

Security controls on servers. Deploy web application firewalls

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	128	0
Non-Labor		0	2,100	0
NSE		0	0	0
	Total	0	2,228	0
FTE		0.0	1.1	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758R - RAMP - Incremental Web Applications and Database Firewalls
Workpaper Detail: 00758R.001 - RAMP - Incremental Security controls on servers. Deploy web application firewalls

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Web Applications and Database Firewalls

Program Description: Security controls on servers. Deploy web application firewalls

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758U - RAMP - Incremental Enterprise Source Code Security

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758U - RAMP - Incremental Enterprise Source Code Security

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	80	36
Non-Labor	Zero-Based	0	0	0	0	0	0	1,100	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	1,180	36
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	0.8	0.4

Business Purpose:

These security systems enhance our ability to support cloud based solutions. Capability to detect security vulnerabilities and exposure prior to production release of code.

Physical Description:

Purchase infrastructure (servers and storage systems) necessary to expand existing source code security scanning system for use across IT developers groups; internal and external third party. The project will have standard interfaces to Source Code Management tool.

Project Justification:

Currently source code security checking is done via developer training and testing at the end of the development cycle. This project integrates the source code security testing into the development process so that problems are identified as they occur so that they can be addressed immediately. This change will reduce the likelihood of a cybersecurity impact due to code vulnerabilities.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758U - RAMP - Incremental Enterprise Source Code Security

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758U**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758U - RAMP - Incremental Enterprise Source Code Security
 Workpaper Detail: 00758U.001 - RAMP - Incremental Proactive preventative application scanning static analysis of source code
 In-Service Date: 03/31/2019

Description:

Self developed software portion of the project

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	80	36
Non-Labor		0	165	0
NSE		0	0	0
	Total	0	245	36
FTE		0.0	0.8	0.4

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758U - RAMP - Incremental Enterprise Source Code Security
 Workpaper Detail: 00758U.001 - RAMP - Incremental Proactive preventative application scanning static analysis of source code bef

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Enterprise Source Code Security

Program Description: Proactive preventative application scanning, static analysis of source code before in house and/or third party software is released into production

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758U - RAMP - Incremental Enterprise Source Code Security
 Workpaper Detail: 00758U.002 - RAMP - Incremental Proactive preventative application scanning static analysis of sour
 In-Service Date: 03/31/2019
 Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		0	935	0
NSE		0	0	0
	Total	0	935	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758U - RAMP - Incremental Enterprise Source Code Security
 Workpaper Detail: 00758U.002 - RAMP - Incremental Proactive preventative application scanning static analysis of source code

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Enterprise Source Code Security

Program Description: Proactive preventative application scanning, static analysis of source code before in house and/or third party software is released into production

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758V - RAMP - Incremental Wired Network Preventative Controls

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758V - RAMP - Incremental Wired Network Preventative Controls

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	175	60
Non-Labor	Zero-Based	0	0	0	0	0	0	3,200	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	3,375	60
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.6

Business Purpose:

Enhanced ability to identify, protect, detect, respond, and recover from a event which results from compromised device connecting to the wired network.

Physical Description:

This project will evaluate current state solutions and deploy a technology which will manage wired network access. In addition to providing network access based upon policy; the project will also integrate this solution with existing systems to automatically remediate malicious or high risk endpoints; it will also provide visability and siutational awareness to the Network Operations Center and Information Security Operations Center

Project Justification:

Prevent unauthorized network access to sensitive networks.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758V - RAMP - Incremental Wired Network Preventative Controls

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758V**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758V - RAMP - Incremental Wired Network Preventative Controls
 Workpaper Detail: 00758V.001 - RAMP - Incremental Impl tech ctrls to authenticate substation devices before granting n
 In-Service Date: 04/30/2019

Description:

Implement technical controls to authenticate substation devices before granting network access

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	175	60
Non-Labor		0	3,200	0
NSE		0	0	0
	Total	0	3,375	60
FTE		0.0	1.0	0.6

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758V - RAMP - Incremental Wired Network Preventative Controls
 Workpaper Detail: 00758V.001 - RAMP - Incremental Impl tech ctrls to authenticate substation devices before granting ntwk access

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Wired Network Preventative Controls

Program Description: Implement technical controls to authenticate substation devices before granting network access

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758W - RAMP - Incremental Multi Factor Authentication Refresh

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758W - RAMP - Incremental Multi Factor Authentication Refresh

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	140	0
Non-Labor	Zero-Based	0	0	0	0	0	0	2,500	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	2,640	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	1.2	0.0

Business Purpose:

Improve access security controls for remote privileged access.

Physical Description:

This project will encompass all of the current MFA implementation as well as servers and cloud offerings. MFA should be rolled out enterprise-wide and should be distributed to all users and vendors.

Project Justification:

Timely replacement with current state multi-factor authentication technology.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758W - RAMP - Incremental Multi Factor Authentication Refresh

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758W**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758W - RAMP - Incremental Multi Factor Authentication Refresh
 Workpaper Detail: 00758W.001 - RAMP - Incremental RSA or another
 In-Service Date: 10/31/2018

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	140	0
Non-Labor		0	375	0
NSE		0	0	0
	Total	0	515	0
FTE		0.0	1.2	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758W - RAMP - Incremental Multi Factor Authentication Refresh
Workpaper Detail: 00758W.001 - RAMP - Incremental RSA or another

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Multi Factor Authentication Refresh

Program Description: RSA or like authentication refresh

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758W - RAMP - Incremental Multi Factor Authentication Refresh
 Workpaper Detail: 00758W.002 - RAMP - Incremental RSA or another
 In-Service Date: 10/31/2018

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	0
Non-Labor		0	2,125	0
NSE		0	0	0
	Total	0	2,125	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758W - RAMP - Incremental Multi Factor Authentication Refresh
 Workpaper Detail: 00758W.002 - RAMP - Incremental RSA or another

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Multi Factor Authentication Refresh

Program Description: RSA or like authentication refresh

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758X - RAMP - Incremental My Account Multi Factor Authentication

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758X - RAMP - Incremental My Account Multi Factor Authentication

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	0	70
Non-Labor	Zero-Based	0	0	0	0	0	0	0	409
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	0	479
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.6

Business Purpose:

- Improved customer account protection and user experience.
- Reduced likelihood of and impact of account takeovers.

Physical Description:

Custom development of 2FA for SCG and SDGE MyAccount applications.

Project Justification:

Increased risk of customer energy usage data breaches due to compromised customer credentials. As 2FA adoption increases across all verticals, customers expect to have the 2FA option to protect their information.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: A. PROTECT
Category-Sub: 1. PROTECT
Workpaper Group: 00758X - RAMP - Incremental My Account Multi Factor Authentication

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758X**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758X - RAMP - Incremental My Account Multi Factor Authentication
 Workpaper Detail: 00758X.001 - RAMP - Incremental My Account two factor authentication
 In-Service Date: 04/30/2019
 Description:

My Account two factor authentication

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	70
Non-Labor		0	0	409
NSE		0	0	0
	Total	0	0	479
FTE		0.0	0.0	0.6

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: A. PROTECT
 Category-Sub: 1. PROTECT
 Workpaper Group: 00758X - RAMP - Incremental My Account Multi Factor Authentication
 Workpaper Detail: 00758X.001 - RAMP - Incremental My Account two factor authentication

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: My Account Multi Factor Authentication

Program Description: My Account two factor authentication

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Protect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Category: B. DETECT
Workpaper: VARIOUS

Summary for Category: B. DETECT

	In 2016\$ (000)			
	Adjusted-Recorded	Adjusted-Forecast		
	2016	2017	2018	2019
Labor	0	453	127	694
Non-Labor	0	5,200	1,350	12,499
NSE	0	0	0	0
Total	0	5,653	1,477	13,193
FTE	0.0	3.7	1.3	6.0

00758AA RAMP - Incremental Threat Response systems

Labor	0	0	0	231
Non-Labor	0	0	0	4,000
NSE	0	0	0	0
Total	0	0	0	4,231
FTE	0.0	0.0	0.0	2.0

00758AB RAMP - Incremental Threat Recovery systems

Labor	0	0	0	231
Non-Labor	0	0	0	3,999
NSE	0	0	0	0
Total	0	0	0	4,230
FTE	0.0	0.0	0.0	2.0

00758D RAMP - Incremental SCG Network Anomaly Detection Phase 1

Labor	0	128	0	0
Non-Labor	0	1,616	0	0
NSE	0	0	0	0
Total	0	1,744	0	0
FTE	0.0	1.0	0.0	0.0

00758F RAMP - Incremental Insider Threat Detection / Prevention

Labor	0	139	0	0
Non-Labor	0	1,704	0	0
NSE	0	0	0	0
Total	0	1,843	0	0
FTE	0.0	1.2	0.0	0.0

00758I RAMP - Incremental SSL Decryption

Labor	0	116	0	0
Non-Labor	0	180	0	0
NSE	0	0	0	0
Total	0	296	0	0
FTE	0.0	1.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Category: B. DETECT
Workpaper: VARIOUS

	In 2016\$ (000)			
	Adjusted-Recorded	Adjusted-Forecast		
	2016	2017	2018	2019
00758L RAMP - Incremental Network Security Monitoring				
Labor	0	70	46	0
Non-Labor	0	1,700	100	0
NSE	0	0	0	0
Total	0	1,770	146	0
FTE	0.0	0.5	0.5	0.0
00758S RAMP - Incremental Perimeter Tap Infrastructure Redesign				
Labor	0	0	81	0
Non-Labor	0	0	1,250	0
NSE	0	0	0	0
Total	0	0	1,331	0
FTE	0.0	0.0	0.8	0.0
00758Z RAMP - Incremental Threat Detection systems				
Labor	0	0	0	232
Non-Labor	0	0	0	4,500
NSE	0	0	0	0
Total	0	0	0	4,732
FTE	0.0	0.0	0.0	2.0

Note: Totals may include rounding differences.

Beginning of Workpaper Group
00758AA - RAMP - Incremental Threat Response systems

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AA - RAMP - Incremental Threat Response systems

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	231	
Non-Labor	Zero-Based	0	0	0	0	0	0	4,000	
NSE	Zero-Based	0	0	0	0	0	0	0	
Total		0	0	0	0	0	0	4,231	
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	2.0	

Business Purpose:

The Cybersecurity Respond function refers to developing and implementing the appropriate activities to take action regarding a detected Cybersecurity event. The Respond Function supports the ability to contain the impact of a potential Cybersecurity event. Examples of control Categories within this Function include: Response Planning; Communications; Analysis; Mitigation and Improvements.

The Incident Response team coordinates cybersecurity incident response activities when a security event is escalated. They also provide analysis of the incident during the incident to determine the most effective response as well as after the incident in terms of lessons learned. During the incident communications with stakeholders are maintained. This functional area is the focus of ongoing training to maintain readiness through exercises to validate the response plans for high impact systems.

Physical Description:

Evaluate and deploy hardware and software systems to improve Cybersecurity Response function capabilities

Project Justification:

- Cost estimated are based on cybersecurity subject matter experts and historical experience responding to changing priorities and risks to address:
- Timely implementation of technology controls
- Addressing evolving threat capabilities
- Supporting and/or leveraging new technologies

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758AA - RAMP - Incremental Threat Response systems

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758AA**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AA - RAMP - Incremental Threat Response systems
 Workpaper Detail: 00758AA.001 - RAMP - Incremental Automated recovery systems cyber threats
 In-Service Date: 11/30/2019

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	231
Non-Labor		0	0	600
NSE		0	0	0
	Total	0	0	831
FTE		0.0	0.0	2.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AA - RAMP - Incremental Threat Response systems
 Workpaper Detail: 00758AA.001 - RAMP - Incremental Automated recovery systems cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Incident Response

Program Description: Vendor solution for forensics infrastructure

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Respond

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AA - RAMP - Incremental Threat Response systems
 Workpaper Detail: 00758AA.002 - RAMP - Incremental Automated response systems cyber threats
 In-Service Date: Not Applicable

Description:

Non self developed software portion of the project.

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	0
Non-Labor		0	0	3,400
NSE		0	0	0
	Total	0	0	3,400
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AA - RAMP - Incremental Threat Response systems
 Workpaper Detail: 00758AA.002 - RAMP - Incremental Automated response systems cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Incident Response

Program Description: Vendor solution for forensics infrastructure

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Respond

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758AB - RAMP - Incremental Threat Recovery systems

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AB - RAMP - Incremental Threat Recovery systems

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	231	
Non-Labor	Zero-Based	0	0	0	0	0	0	3,999	
NSE	Zero-Based	0	0	0	0	0	0	0	
Total		0	0	0	0	0	0	4,230	
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	2.0	

Business Purpose:

The Cybersecurity Recover function refers to developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a Cybersecurity event. Examples of control Categories within this Function include: Recovery Planning; Improvements and Communications. The Recover Function is a core capability of the Information Technology business unit. The Cybersecurity department's focus on Recovery functions is to maintain resilience against a Cybersecurity event and, if necessary, to restore cybersecurity capabilities to a known state after an incident.

Physical Description:

Evaluate and deploy hardware and software systems to improve Cybersecurity Recover function capabilities

Project Justification:

- Cost estimated are based on cybersecurity subject matter experts and historical experience responding to changing priorities and risks to address:
- Timely implementation of technology controls
- Addressing evolving threat capabilities
- Supporting and/or leveraging new technologies

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758AB - RAMP - Incremental Threat Recovery systems

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758AB**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AB - RAMP - Incremental Threat Recovery systems
 Workpaper Detail: 00758AB.001 - RAMP - Incremental Automated recovery systems cyber threats
 In-Service Date: 11/30/2019

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	231
Non-Labor		0	0	600
NSE		0	0	0
	Total	0	0	831
FTE		0.0	0.0	2.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AB - RAMP - Incremental Threat Recovery systems
 Workpaper Detail: 00758AB.001 - RAMP - Incremental Automated recovery systems cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Security capability recovery infrastructure

Program Description: Recovery infrastructure specific to security capability infrastructure

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Recover

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AB - RAMP - Incremental Threat Recovery systems
 Workpaper Detail: 00758AB.002 - RAMP - Incremental Automated recovery systems cyber threats
 In-Service Date: Not Applicable

Description:

Non self developed software portion of the project.

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		0	0	3,399
NSE		0	0	0
	Total	0	0	3,399
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758AB - RAMP - Incremental Threat Recovery systems
 Workpaper Detail: 00758AB.002 - RAMP - Incremental Automated recovery systems cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Security capability recovery infrastructure

Program Description: Recovery infrastructure specific to security capability infrastructure

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Recover

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758D - RAMP - Incremental SCG Network Anomaly Detection Phase 1

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758D - RAMP - Incremental SCG Network Anomaly Detection Phase 1

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	128	0	0
Non-Labor	Zero-Based	0	0	0	0	0	1,616	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	1,744	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0

Business Purpose:

- New capability to identify, respond and recover from a cyber incident in critical SoCalGas SCADA/ICS networks
 - Provide SCG operators visibility into infrastructure configuration and performance
 - Provide network operations visibility into network flows
 - Analytic platform will provide ability to visualize network flows, potential security or misconfigurations
- Limit impact of cyber security incidents on the gas grid
 Reduce identification of indicators of compromise within SCG's most critical networks/environments
 Reduce recover times during a cyber security incident

Physical Description:

Deployment of company standard network anomaly devices to critical SCG ICS SCADA infrastructure. Deployment of these devices will focus on key gas control transmission locations and compressor stations. The project will integrate this new technology into SCG logging infrastructure and security incident and event monitoring solutions so events and alerts can be viewed and responded to by Security Operations Center (SOC).

Project Justification:

Provides visibility into ICS/SCADA network traffic to detect anomalies due to configurations issues or unauthorized activity.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758D - RAMP - Incremental SCG Network Anomaly Detection Phase 1

Forecast Methodology:

Labor - Zero-Based

Project is currently in-flight. Based on actual timeline of the project to complete.

Non-Labor - Zero-Based

Project is currently in-flight. Based on actual timeline of the project to complete.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758D**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758D - RAMP - Incremental SCG Network Anomaly Detection Phase 1
 Workpaper Detail: 00758D.001 - RAMP - Incremental SCG Network Anomaly Detection Phase 1
 In-Service Date: 08/31/2017

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		128	0	0
Non-Labor		240	0	0
NSE		0	0	0
	Total	368	0	0
FTE		1.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758D - RAMP - Incremental SCG Network Anomaly Detection Phase 1
 Workpaper Detail: 00758D.001 - RAMP - Incremental SCG Network Anomaly Detection Phase 1

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Cyber Security

Program Description: SCG Network Anomaly Detection Phase 1

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758D - RAMP - Incremental SCG Network Anomaly Detection Phase 1
 Workpaper Detail: 00758D.002 - RAMP - Incremental Deploy Silent Defense SCADA ICS protection SCG critical sites
 In-Service Date: 08/31/2017

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	0
Non-Labor		1,376	0	0
NSE		0	0	0
	Total	1,376	0	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758D - RAMP - Incremental SCG Network Anomaly Detection Phase 1
 Workpaper Detail: 00758D.002 - RAMP - Incremental Deploy Silent Defense SCADA ICS protection SCG critical sites

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Cyber Security

Program Description: SCG Network Anomaly Detection Phase 1

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758F - RAMP - Incremental Insider Threat Detection / Prevention

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758F - RAMP - Incremental Insider Threat Detection / Prevention

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	139	0	0
Non-Labor	Zero-Based	0	0	0	0	0	1,704	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	1,843	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.2	0.0	0.0

Business Purpose:

The Cybersecurity Detect functions refers to developing and implementing the appropriate activities to identify the occurrence of a Cybersecurity event. The Detect Function enables timely discovery of Cybersecurity events. Examples of control Categories within this Function include: Anomalies and Events; Security Continuous Monitoring and Detection Processes.

Timely discovery of Cybersecurity events is enabled by monitoring security-related activities in systems and applications, anomaly detection and security event detection and escalation. The 7x24 Information Security Operations Center monitors detection infrastructure systems to investigate security events. If the security events have the potential to impact the organization, they are escalated to the security incident response process.

Physical Description:

Deployment of new user behavior and network activity anomaly detection technologies and enhancements of existing security technologies already in production on the corporate network.

Project Justification:

Improves the capability to detect anomalous activity by insiders

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758F - RAMP - Incremental Insider Threat Detection / Prevention

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758F**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758F - RAMP - Incremental Insider Threat Detection / Prevention
 Workpaper Detail: 00758F.001 - RAMP - Incremental User behavior analytics / MS Advanced Threat Analysis machine learn
 In-Service Date: 10/31/2017

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		139	0	0
Non-Labor		256	0	0
NSE		0	0	0
	Total	395	0	0
FTE		1.2	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758F - RAMP - Incremental Insider Threat Detection / Prevention
 Workpaper Detail: 00758F.001 - RAMP - Incremental User behavior analytics / MS Advanced Threat Analysis machine learning, be

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Threat Detection

Program Description: Insider Threat Detection / Prevention

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758F - RAMP - Incremental Insider Threat Detection / Prevention
 Workpaper Detail: 00758F.002 - RAMP - Incremental Outlook Enterprise Threat Intel system
 In-Service Date: 10/31/2017
 Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		1,448	0	0
NSE		0	0	0
	Total	1,448	0	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758F - RAMP - Incremental Insider Threat Detection / Prevention
 Workpaper Detail: 00758F.002 - RAMP - Incremental Outlook Enterprise Threat Intel system

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Threat Detection

Program Description: Insider Threat Detection / Prevention

Risk/Mitigation:

Risk: A major cyber security incident that causes dirup

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758I - RAMP - Incremental SSL Decryption

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758I - RAMP - Incremental SSL Decryption

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	116	0	0
Non-Labor	Zero-Based	0	0	0	0	0	180	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	296	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0

Business Purpose:

Improved visibility into encrypted traffic will help us to better identify compromised hosts and prevent: corporate data loss, misconfiguration among all endpoints, insider threats, phishing and spear-phishing attempts and compromises. The decryption ability will allow us to inspect the data.

Physical Description:

This project will implement the technology to allow the inspection of encrypted data. The technology will be implemented at the perimeters in the datacenters. Traffic will be inspected by multiple IS tools, IPS, Malware detection, antivirus, data loss prevention and passive vulnerability detection to ensure full inspection.

Project Justification:

Improve visibility into encrypted network data will decrease our ability to identify malicious activity within our environment.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758I - RAMP - Incremental SSL Decryption

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758I**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758I - RAMP - Incremental SSL Decryption
 Workpaper Detail: 00758I.001 - RAMP - Incremental Decrypt SSL at the perimeter to enable inspection
 In-Service Date: 09/30/2017

Description:

Decrypt SSL at the perimeter to enable inspection

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		116	0	0
Non-Labor		180	0	0
NSE		0	0	0
	Total	296	0	0
FTE		1.0	0.0	0.0

Note: Totals may include rounding differences.

Beginning of Workpaper Group
00758L - RAMP - Incremental Network Security Monitoring

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758L - RAMP - Incremental Network Security Monitoring

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	70	46	0
Non-Labor	Zero-Based	0	0	0	0	0	1,700	100	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	1,770	146	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.5	0.5	0.0

Business Purpose:

The Cybersecurity Detect function refers to developing and implementing the appropriate activities to identify the occurrence of a Cybersecurity event. The Detect Function enables timely discovery of Cybersecurity events. Examples of control Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes. Timely discovery of Cybersecurity events is enabled by monitoring security-related activities in systems and applications, anomaly detection, and security event detection and escalation. The 7x24 Information Security Operations Center monitors detection infrastructure systems to investigate security events. If the security events have the potential to impact the organization they are escalated to the security incident response process.

Physical Description:

Deploy a hardware and software system to consolidate network security data from existing network security controls on the business network, and deploy new capabilities on the business network to support network flow, packet meta data, and full packet capture.

Project Justification:

Will improve network security detection capabilities by providing a broader more complete view of the activities within the environment.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758L - RAMP - Incremental Network Security Monitoring

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758L**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758L - RAMP - Incremental Network Security Monitoring
 Workpaper Detail: 00758L.001 - RAMP - Incremental i.e. Packet Sled Splunk Threat Analytics
 In-Service Date: 04/30/2018

Description:

Self developed software portion of the project

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		70	46	0
Non-Labor		255	100	0
NSE		0	0	0
	Total	325	146	0
FTE		0.5	0.5	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758L - RAMP - Incremental Network Security Monitoring
Workpaper Detail: 00758L.001 - RAMP - Incremental i.e. Packet Sled Splunk Threat Analytics

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Network Security Monitoring

Program Description: Packet Sled, Splunk & Threat Analytics

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758L - RAMP - Incremental Network Security Monitoring
 Workpaper Detail: 00758L.002 - RAMP - Incremental Packet Sled Splunk Threat Analytics - non SDS
 In-Service Date: 04/30/2018
 Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		1,445	0	0
NSE		0	0	0
	Total	1,445	0	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758L - RAMP - Incremental Network Security Monitoring
 Workpaper Detail: 00758L.002 - RAMP - Incremental Packet Sled Splunk Threat Analytics - non SDS

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Network Security Monitoring

Program Description: Packet Sled, Splunk & Threat Analytics

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758S - RAMP - Incremental Perimeter Tap Infrastructure Redesign

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758S - RAMP - Incremental Perimeter Tap Infrastructure Redesign

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	81	0
Non-Labor	Zero-Based	0	0	0	0	0	0	1,250	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	1,331	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	0.8	0.0

Business Purpose:

Simplified network design that allows more efficient and quicker response to integrate needed tools or bypass tools to assist in troubleshooting. Increased visibility and log collection to provide a more holistic view of risk, security posture, and network insight.

Physical Description:

Deploy new network tap infrastructure within the datacenter perimeters. The new solution will be inline and provide the ability to both flow the traffic inline through security and network tools, bypass said tools and connect tools for passive detection and collection.

Project Justification:

Improved network capacity and reliability in support of increased network complexity as additional security tools are implemented such as inline DLP MTAs and Web Application Firewalls.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758S - RAMP - Incremental Perimeter Tap Infrastructure Redesign

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758S**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758S - RAMP - Incremental Perimeter Tap Infrastructure Redesign
 Workpaper Detail: 00758S.001 - RAMP - Incremental Improved passive and by-pass tap technology
 In-Service Date: 06/30/2018

Description:

Improved passive and by-pass tap technology

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	81	0
Non-Labor		0	1,250	0
NSE		0	0	0
	Total	0	1,331	0
FTE		0.0	0.8	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758S - RAMP - Incremental Perimeter Tap Infrastructure Redesign
 Workpaper Detail: 00758S.001 - RAMP - Incremental Improved passive and by-pass tap technology

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Perimeter Tap Infrastructure Redesign

Program Description: Improved passive and by-pass tap technology

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758Z - RAMP - Incremental Threat Detection systems

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	232	
Non-Labor	Zero-Based	0	0	0	0	0	0	4,500	
NSE	Zero-Based	0	0	0	0	0	0	0	
Total		0	0	0	0	0	0	4,732	
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	2.0	

Business Purpose:

The Cybersecurity Detect function refers to developing and implementing the appropriate activities to identify the occurrence of a Cybersecurity event. The Detect Function enables timely discovery of Cybersecurity events. Examples of control Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes. Timely discovery of Cybersecurity events is enabled by monitoring security-related activities in systems and applications, anomaly detection, and security event detection and escalation. The 7x24 Information Security Operations Center monitors detection infrastructure systems to investigate security events. If the security events have the potential to impact the organization, they are escalated to the security incident response process.

Physical Description:

Evaluate and deploy hardware and software systems to improve threat detection capabilities

Project Justification:

- Cost estimated are based on cybersecurity subject matter experts and historical experience responding to changing priorities and risks to address:
- Timely implementation of technology controls
- Addressing evolving threat capabilities
- Supporting and/or leveraging new technologies

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: B. DETECT
Category-Sub: 1. DETECT
Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758Z**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems
 Workpaper Detail: 00758Z.001 - RAMP - Incremental Automated detection systems cyber threats
 In-Service Date: 11/30/2019

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	232
Non-Labor		0	0	675
NSE		0	0	0
	Total	0	0	907
FTE		0.0	0.0	2.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems
 Workpaper Detail: 00758Z.001 - RAMP - Incremental Automated detection systems cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Cybersecurity Event Monitoring - IT

Program Description: Threat Detection systems

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems
 Workpaper Detail: 00758Z.002 - RAMP - Incremental Automated detection systems cyber threats
 In-Service Date: 11/30/2019
 Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		0	0	3,825
NSE		0	0	0
	Total	0	0	3,825
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems
 Workpaper Detail: 00758Z.002 - RAMP - Incremental Automated detection systems cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Cybersecurity Event Monitoring – IT

Program Description: Threat Detection systems

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems
 Workpaper Detail: 00758Z.003 - RAMP - Incremental automated detection systems cyber threats
 In-Service Date: 11/30/2019

Description:

automated detection systems cyber threats

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		0	0	0
NSE		0	0	0
	Total	0	0	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems
 Workpaper Detail: 00758Z.003 - RAMP - Incremental automated detection systems cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Cybersecurity Event Monitoring – IT

Program Description: Threat Detection systems

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems
 Workpaper Detail: 00758Z.004 - RAMP - Incremental automated detection systems cyber threats
 In-Service Date: 11/30/2019

Description:

automated detection systems cyber threats

Forecast In 2016 \$(000)					
	Years	2017	2018	2019	
Labor		0	0	0	
Non-Labor		0	0	0	
NSE		0	0	0	
	Total	0	0	0	
FTE		0.0	0.0	0.0	

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: B. DETECT
 Category-Sub: 1. DETECT
 Workpaper Group: 00758Z - RAMP - Incremental Threat Detection systems
 Workpaper Detail: 00758Z.004 - RAMP - Incremental automated detection systems cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Cybersecurity Event Monitoring – IT

Program Description: Threat Detection systems

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Detect

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Category: C. RESPOND
Workpaper: VARIOUS

Summary for Category: C. RESPOND

	In 2016\$ (000)			
	Adjusted-Recorded	Adjusted-Forecast		
	2016	2017	2018	2019
Labor	0	52	163	0
Non-Labor	0	150	1,751	0
NSE	0	0	0	0
Total	0	202	1,914	0
FTE	0.0	0.5	1.5	0.0

00758C RAMP - Incremental Forensics System Rebuild

Labor	0	52	0	0
Non-Labor	0	150	0	0
NSE	0	0	0	0
Total	0	202	0	0
FTE	0.0	0.5	0.0	0.0

00758T RAMP - Incremental Incident Response Secure Collaboration

Labor	0	0	163	0
Non-Labor	0	0	1,751	0
NSE	0	0	0	0
Total	0	0	1,914	0
FTE	0.0	0.0	1.5	0.0

Note: Totals may include rounding differences.

Beginning of Workpaper Group
00758C - RAMP - Incremental Forensics System Rebuild

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: C. RESPOND
 Category-Sub: 1. RESPOND
 Workpaper Group: 00758C - RAMP - Incremental Forensics System Rebuild

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	52	0	0
Non-Labor	Zero-Based	0	0	0	0	0	150	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	202	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.5	0.0	0.0

Business Purpose:

The enterprise Forensics system is at end of life and no longer supported by manufacturer. Legal departments at Sempra Corp, SDGE and SCG are the primary drivers of investigation requests.

Physical Description:

This project will replace the legacy system with new upgraded servers and storage forensics system and expand our capabilities for e-discovery (electronic discovery of relevant files). The system is autonomous, dedicated servers / storage within a secure Forensics zone not accessible from the corporate network to meet Legal, security and privacy requirements and for this reason the system cannot utilize shared VM / SAN infrastructure. This project will implement replication and restore capabilities.

Project Justification:

Maintaining in house forensics capability in support of Legal and HR departments, and expanding e-discovery capability will avoid cost prohibitive third party services and provide more robust recoverability of the data storage system.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: C. RESPOND
Category-Sub: 1. RESPOND
Workpaper Group: 00758C - RAMP - Incremental Forensics System Rebuild

Forecast Methodology:

Labor - Zero-Based

Project is currently in-flight. Based on actual timeline of the project to complete.

Non-Labor - Zero-Based

Project is currently in-flight. Based on actual timeline of the project to complete.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758C**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: C. RESPOND
 Category-Sub: 1. RESPOND
 Workpaper Group: 00758C - RAMP - Incremental Forensics System Rebuild
 Workpaper Detail: 00758C.001 - RAMP - Incremental Forensics System Rebuild
 In-Service Date: 03/31/2017

Description:

...

Forecast In 2016 \$(000)				
Years		<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		52	0	0
Non-Labor		150	0	0
NSE		0	0	0
	Total	202	0	0
FTE		0.5	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: C. RESPOND
 Category-Sub: 1. RESPOND
 Workpaper Group: 00758C - RAMP - Incremental Forensics System Rebuild
 Workpaper Detail: 00758C.001 - RAMP - Incremental Forensics System Rebuild

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Enterprise Forensics

Program Description: Rebuild of the forensics and ediscovery systems

Risk/Mitigation:

Risk: All Cyber Risks

Mitigation: Respond

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758T - RAMP - Incremental Incident Response Secure Collaboration

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: C. RESPOND
 Category-Sub: 1. RESPOND
 Workpaper Group: 00758T - RAMP - Incremental Incident Response Secure Collaboration

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Years									
Labor	Zero-Based	0	0	0	0	0	0	163	0
Non-Labor	Zero-Based	0	0	0	0	0	0	1,751	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	1,914	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	1.5	0.0

Business Purpose:

The Cybersecurity Respond function refers to developing and implementing the appropriate activities to take action regarding a detected Cybersecurity event. The Respond Function supports the ability to contain the impact of a potential Cybersecurity event. Examples of control Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

The Incident Response team coordinates cybersecurity incident response activities when a security event is escalated. They also provide analysis of the incident, during the incident, to determine the most effective response, as well as after the incident in terms of lessons learned. During the incident, communications with stakeholders are maintained. This functional area is the focus of ongoing training to maintain readiness through exercises to validate the response plans for high impact systems.

Physical Description:

Deploy a new security platform for Incident Response collaboration on large scale cyber events.

Project Justification:

Improve the ability to respond to large scale cyber incident.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: C. RESPOND
Category-Sub: 1. RESPOND
Workpaper Group: 00758T - RAMP - Incremental Incident Response Secure Collaboration

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758T**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: C. RESPOND
 Category-Sub: 1. RESPOND
 Workpaper Group: 00758T - RAMP - Incremental Incident Response Secure Collaboration
 Workpaper Detail: 00758T.001 - RAMP - Incremental Deploy a comm and coordination platform securely leveraged on the c
 In-Service Date: 09/30/2018

Description:

Self developed software portion of the project

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	163	0
Non-Labor		0	263	0
NSE		0	0	0
	Total	0	426	0
FTE		0.0	1.5	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: C. RESPOND
Category-Sub: 1. RESPOND
Workpaper Group: 00758T - RAMP - Incremental Incident Response Secure Collaboration
Workpaper Detail: 00758T.001 - RAMP - Incremental Deploy a comm and coordination platform securely leveraged on the corp ntw

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Incident Response Secure Collaboration

Program Description: Deploy a communication and coordination platform that can be securely leveraged on the corporate network

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Respond

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: C. RESPOND
 Category-Sub: 1. RESPOND
 Workpaper Group: 00758T - RAMP - Incremental Incident Response Secure Collaboration
 Workpaper Detail: 00758T.002 - RAMP - Incremental Deploy a comm and coordination platform securely leveraged on the co
 In-Service Date: 09/30/2018
 Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		0	1,488	0
NSE		0	0	0
	Total	0	1,488	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: C. RESPOND
 Category-Sub: 1. RESPOND
 Workpaper Group: 00758T - RAMP - Incremental Incident Response Secure Collaboration
 Workpaper Detail: 00758T.002 - RAMP - Incremental Deploy a comm and coordination platform securely leveraged on the corp ntwk

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Incident Response Secure Collaboration

Program Description: Deploy a communication and coordination platform that can be securely leveraged on the Corporate Network

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Respond

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Category: D. IDENTIFY
Workpaper: VARIOUS

Summary for Category: D. IDENTIFY

	In 2016\$ (000)			
	Adjusted-Recorded	Adjusted-Forecast		
	2016	2017	2018	2019
Labor	0	174	0	231
Non-Labor	0	1,300	0	4,500
NSE	0	0	0	0
Total	0	1,474	0	4,731
FTE	0.0	1.5	0.0	2.0

00758E RAMP - Incremental Enterprise Threat Intelligence

Labor	0	174	0	0
Non-Labor	0	1,300	0	0
NSE	0	0	0	0
Total	0	1,474	0	0
FTE	0.0	1.5	0.0	0.0

00758Y RAMP - Incremental Threat Identification systems

Labor	0	0	0	231
Non-Labor	0	0	0	4,500
NSE	0	0	0	0
Total	0	0	0	4,731
FTE	0.0	0.0	0.0	2.0

Note: Totals may include rounding differences.

Beginning of Workpaper Group
00758E - RAMP - Incremental Enterprise Threat Intelligence

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758E - RAMP - Incremental Enterprise Threat Intelligence

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
	Years								
Labor	Zero-Based	0	0	0	0	0	174	0	0
Non-Labor	Zero-Based	0	0	0	0	0	1,300	0	0
NSE	Zero-Based	0	0	0	0	0	0	0	0
	Total	0	0	0	0	0	1,474	0	0
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	1.5	0.0	0.0

Business Purpose:

- Expand our ability to identify, react, respond quickly, and recover from a sensitive information extraction and cyber security incident.
- Reduced time to respond to threats and incidents.
- Improved efficiency and resource utilization.
- Sharing threat intelligence from government agencies and trusted authorities.

Limit potential liability damage a cyber security incident
 Ability to leverage this technology for future requirements

Physical Description:

Acquire and deploy a solution from a top tier provider of Threat Intelligence, Analysis, Cyber Espionage, Scenario Testing and Automated Response.

Project Justification:

Improve capability to response effectively to cyber incidents effecting critical infrastructure and enterprise systems.

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: D. IDENTIFY
Category-Sub: 1. IDENTIFY
Workpaper Group: 00758E - RAMP - Incremental Enterprise Threat Intelligence

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758E**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758E - RAMP - Incremental Enterprise Threat Intelligence
 Workpaper Detail: 00758E.001 - RAMP - Incremental Enterprise Threat Intel system
 In-Service Date: 06/30/2017

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		174	0	0
Non-Labor		195	0	0
NSE		0	0	0
	Total	369	0	0
FTE		1.5	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758E - RAMP - Incremental Enterprise Threat Intelligence
 Workpaper Detail: 00758E.001 - RAMP - Incremental Enterprise Threat Intel system

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Vulnerability Management

Program Description: Implementation of an active scanning vulnerability management solution and a passive scanning capability

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Identify

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758E - RAMP - Incremental Enterprise Threat Intelligence
 Workpaper Detail: 00758E.002 - RAMP - Incremental Enterprise Threat Intel system
 In-Service Date: 06/30/2017

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		1,105	0	0
NSE		0	0	0
	Total	1,105	0	0
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758E - RAMP - Incremental Enterprise Threat Intelligence
 Workpaper Detail: 00758E.002 - RAMP - Incremental Enterprise Threat Intel system

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Vulnerability Management

Program Description: Implementation of an active scanning vulnerability management solution and a passive scanning

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Identify

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Beginning of Workpaper Group
00758Y - RAMP - Incremental Threat Identification systems

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758Y - RAMP - Incremental Threat Identification systems

Summary of Results (Constant 2016 \$ in 000s):

Forecast Method		Adjusted Recorded					Adjusted Forecast		
		2012	2013	2014	2015	2016	2017	2018	2019
Labor	Zero-Based	0	0	0	0	0	0	0	231
Non-Labor	Zero-Based	0	0	0	0	0	0	0	4,500
NSE	Zero-Based	0	0	0	0	0	0	0	0
Total		0	0	0	0	0	0	0	4,731
FTE	Zero-Based	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.0

Business Purpose:

The Cybersecurity Identify function refers to developing organizational understanding to manage Cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the NIST Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks, enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of control Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy. Program activities in the Identify Function include maintaining a security policy framework, asset management, risk assessments, threat intelligence, and risk management. For example, in conjunction with the IT Enterprise Architecture group, the Cybersecurity control capabilities are documented. Risk assessments conducted by internal and external resources review the security posture of practices, technology, security controls, and other business activities. The assessments identify opportunities for improvements. These opportunities are prioritized via the risk management process. As projects are identified, funded, and completed, the security capabilities are updated in the capability repository.

Physical Description:

Evaluate and deploy hardware and software systems to improve cybersecurity identify function capabilities.

Project Justification:

- Cost estimated are based on cybersecurity subject matter experts and historical experience responding to changing priorities and risks to address:
- Timely implementation of technology controls
- Addressing evolving threat capabilities
- Supporting and/or leveraging new technologies

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
Witness: Gavin H. Worden
Budget Code: 00758.0
Category: D. IDENTIFY
Category-Sub: 1. IDENTIFY
Workpaper Group: 00758Y - RAMP - Incremental Threat Identification systems

Forecast Methodology:

Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

Non-Labor - Zero-Based

Based on Project Manager and Subject Matter Expert estimates.

NSE - Zero-Based

N/A

**Beginning of Workpaper Sub Details for
Workpaper Group 00758Y**

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758Y - RAMP - Incremental Threat Identification systems
 Workpaper Detail: 00758Y.001 - RAMP - Incremental Identify cyber threats
 In-Service Date: 11/30/2019

Description:

Self developed software portion of the project
--

Forecast In 2016 \$(000)				
	Years	<u>2017</u>	<u>2018</u>	<u>2019</u>
Labor		0	0	231
Non-Labor		0	0	675
NSE		0	0	0
	Total	0	0	906
FTE		0.0	0.0	2.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758Y - RAMP - Incremental Threat Identification systems
 Workpaper Detail: 00758Y.001 - RAMP - Incremental Identify cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Threat Identification systems

Program Description: Threat Identification systems

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Identify

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation:

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758Y - RAMP - Incremental Threat Identification systems
 Workpaper Detail: 00758Y.002 - RAMP - Incremental Identify cyber threats
 In-Service Date: 11/30/2019

Description:

License/materials purchase non SDS

Forecast In 2016 \$(000)				
	Years	2017	2018	2019
Labor		0	0	0
Non-Labor		0	0	3,825
NSE		0	0	0
	Total	0	0	3,825
FTE		0.0	0.0	0.0

Note: Totals may include rounding differences.

Southern California Gas Company
2019 GRC - APP
Capital Workpapers

Area: CYBER SECURITY
 Witness: Gavin H. Worden
 Budget Code: 00758.0
 Category: D. IDENTIFY
 Category-Sub: 1. IDENTIFY
 Workpaper Group: 00758Y - RAMP - Incremental Threat Identification systems
 Workpaper Detail: 00758Y.002 - RAMP - Incremental Identify cyber threats

RAMP Item # 1

RAMP Chapter: SCG-3

Program Name: Threat Identification systems

Program Description: Threat Identification systems

Risk/Mitigation:

Risk: A major cyber security incident that causes disrupt

Mitigation: Identify

Forecast CPUC Cost Estimates (\$000)

	<u>2017</u>	<u>2018</u>	<u>2019</u>
Low	0	0	0
High	0	0	0

Funding Source: CPUC-GRC

Forecast Method: Zero-Based

Work Type: Non-Mandated

Work Type Citation: See Workpaper

Historical Embedded Cost Estimates (\$000)

Embedded Costs: 0

Explanation: