

**2016 Risk Assessment Mitigation Phase  
Investigation 16-10-016  
Workpapers to  
Cyber Security  
(Chapter SCG-3-WP)**

January 2017



[illegible]

2016 Risk Assessment Mitigation Phase  
SCG-03-WP  
Risk: Cyber Security (O&M)

Line No.	Mitigation	Project/Program	Project/Program Description	Status	Recorded (Directs, 2015 \$000)					Forecast Range (Directs, 2015 \$000)						Forecast Methodology
					2011	2012	2013	2014	2015	2017 Low	2017 High	2018 Low	2018 High	2019 Low	2019 High	
22		Data Exfiltration	Data Loss Prevention - solution deployment to secure sensitive information egress for enterprise client end points, Mobile Data Terminals (MDTs), Customer Call Center (CCC)	B	-	-	-	-	-	-	-	-	-	-	-	
23		Malware Defenses	End Point Security - enterprise deployment of advanced, non-signature based, malware protection / prevention and analytics	B	-	-	-	-	-	-	-	-	-	-	-	
24		Email and Web Browser Protections	Solution deployment for internet email spam, phishing and malware filtering	B	-	-	-	-	-	-	-	-	-	-	-	
25		Security Small Capital Projects	Operations and reliability expenses associated with blanket work orders for replacement of failed IS production hardware and systems as necessary	B	-	-	-	-	-	-	-	-	-	-	-	
26		Converged Perimeter Systems		P						-	-	-	-	-	-	
27		Host Based Protection		P						-	-	-	-	-	-	
28		IS Zone Rebuild	Replace switches and Intrusion Prevention Systems (IPS) IS zone	P						-	-	-	-	-	-	
29		Web Applications and Database Firewalls	Security controls on servers. Deploy web application firewalls	P						-	-	-	-	-	-	
30		Enterprise Source Code Security	Proactive preventative application scanning, static analysis of source code before in house and/or third party software is released into production	P						-	-	-	-	-	-	
31		Wired Network Preventative Controls	Implement technical controls to authenticate substation devices before granting network access	P						-	-	-	-	-	-	
32		Multi Factor Authentication Refresh	single use token product or another similar solution	P						-	-	-	-	-	-	
33		My Account Multi Factor Authentication		P						-	-	-	-	-	-	
34		Protective Capability infrastructure		P						-	-	-	-	-	-	
35	<b>Protect Subtotal</b>				-	-	376	421	404	464	674	404	704	404	1,064	
36	Detect	O&M GRC - Historical	Base business historical information	B	-	-	1	0	0	-	-	-	-	-	-	
37		O&M Non-Labor Forecast	Forecast for existing employees non-labor costs	B	-	-	-	-	-	-	-	-	-	-	-	
38		O&M Labor Forecast	Forecast for existing employees labor costs	B	-	-	-	-	-	(0)	(0)	(0)	(0)	(0)	(0)	Base Year
39		O&M new FTEs	Forecast for new FTEs	P						-	150	-	150	-	150	Base Year
40		O&M IS Associate Program	Forecast for new IS Associate Program	P						-	-	-	-	-	-	
41		Enterprise Logging Infrastructure	Enterprise log management system deployment	B	-	-	-	-	-	-	-	-	-	-	-	
42		Cyber Security Event Monitoring	Security Event/Incident Management (SEIM) consolidation into enterprise log management solution	B	-	-	-	-	-	-	-	-	-	-	-	
43		HTTPS Egress Decryption	Decrypt Secure Socket Layer (SSL) traffic at the perimeter to enable inspection	P						-	-	-	-	-	-	
44		Network Security Monitoring	Includes activities such as Packet Sled, Splunk, Threat Analytics	P						-	-	-	-	-	-	
45		Perimeter Tap Infrastructure Redesign	improved passive and by-pass tap technology	P						-	-	-	-	-	-	
46		Logging and monitoring infrastructure	Logging and monitoring infrastructure	P						-	-	-	-	-	-	
47	<b>Detect Subtotal</b>				-	-	1	0	0	(0)	150	(0)	150	(0)	150	

2016 Risk Assessment Mitigation Phase  
SCG-03-WP  
Risk: Cyber Security (O&M)

Line No.	Mitigation	Project/Program	Project/Program Description	Status	Recorded (Directs, 2015 \$000)					Forecast Range (Directs, 2015 \$000)						Forecast Methodology
					2011	2012	2013	2014	2015	2017 Low	2017 High	2018 Low	2018 High	2019 Low	2019 High	
48	Respond	O&M GRC - Historical	Base business historical information	B	-	-	16	16	14	-	-	-	-	-	-	
49		O&M Non-Labor Forecast	Forecast for existing employees non-labor costs	B	-	-	-	-	-	-	-	-	-	-	-	
50		O&M Labor Forecast	Forecast for existing employees labor costs	B	-	-	-	-	-	14	14	14	14	14	14	Base Year
51		O&M new FTEs	Forecast for new FTEs	P						-	150	-	150	-	150	Base Year
52		O&M IS Associate Program	Forecast for new IS Associate Program	P						-	-	60	60	-	-	Base Year
53		Incident Response	Vendor solution for forensics infrastructure	B	-	-	-	-	-	-	-	-	-	-	-	
54		Enterprise Forensics	Rebuild of the forensics and ediscovery systems	B	-	-	-	-	-	-	-	-	-	-	-	
55		Security Orchestration	Automate key security triage tasks	P						-	-	-	-	-	-	
56		Incident Response Secure Collaboration	Deploy a communication and coordination platform that can be securely leveraged on the corporate network	P						-	-	-	-	-	-	
57		Incident Response Infrastructure		P						-	-	-	-	-	-	
58	<b>Respond Subtotal</b>				-	-	16	16	14	14	164	74	224	14	164	
59	Recover	O&M GRC - Historical	Base business historical information	B	-	-	2	0	(0)	-	-	-	-	-	-	
60		O&M Non-Labor Forecast	Forecast for existing employees non-labor costs	B	-	-	-	-	-	-	-	-	-	-	-	
61		O&M Labor Forecast	Forecast for existing employees labor costs	B	-	-	-	-	-	(0)	(0)	(0)	(0)	(0)	(0)	Base Year
62		O&M new FTEs	Forecast for new FTEs	P						-	-	-	-	-	-	
63		O&M IS Associate Program	Forecast for new IS Associate Program	P						-	-	-	-	-	-	
64		Security capability recovery infrastructure	Recovery infrastructure specific to security capability infrastructure	P						-	-	-	-	-	-	
65	<b>Recover Subtotal</b>				-	-	2	0	(0)	(0)	(0)	(0)	(0)	(0)	(0)	
66	<b>TOTAL</b>				\$ -	\$ -	\$ 447	\$ 463	\$ 465	\$ 524	\$ 1,034	\$ 524	\$ 1,484	\$ 524	\$ 1,934	

Notes:

- Baseline (B) and Proposed (P).
- Numbers in risk chapter tables may differ due to rounding.
- The purpose of Risk Assessment Mitigation Phase (RAMP) is not to request funding. Any funding requests will be made in the General Rate Case (GRC). The forecasts for mitigations are not for funding purposes, but are rather to provide a range for the future GRC filing. This range will be refined with supporting testimony in the GRC.

Line No.	Mitigation	Project/Program	Project/Program Description	Recorded (Directs, 2015 \$000)						Forecast Range (Directs, 2015 \$000)						2017-2019 Low (Sum)	2017-2019 High (Sum)	Forecast Methodology
				Status	2011	2012	2013	2014	2015	2017 Low	2017 High	2018 Low	2018 High	2019 Low	2019 High			
1	Identify	O&M General Rate Case (GRC) - Historical	Base business historical information	B	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -		
2		O&M Non-Labor Forecast	Forecast for existing employees' non-labor costs	B	-	-	-	-	-	-	-	-	-	-	-	-		
3		O&M Labor Forecast	Forecast for existing employees' labor costs	B	-	-	-	-	-	-	-	-	-	-	-	-		
4		O&M new Full Time Equivalents (FTEs)	Forecast for new FTEs	P														
5		O&M Information Security (IS) Associate Program	Forecast for new IS Associate Program	P														
6		Vulnerability Management	Implementation of an active scanning vulnerability management solution and a passive scanning capability	B	-	-	379	(20)	-									
7		Asset and Risk management infrastructure	Asset management, threat intelligence, vulnerability management	P														
8	Identify Subtotal				-	-	379	(20)	-									
9	Protect	O&M GRC - Historical	Base business historical information	B	-	-	-	-	-	-	-	-	-	-	-	-		
10		O&M Non-Labor Forecast	Forecast for existing employees non-labor costs	B	-	-	-	-	-	-	-	-	-	-	-	-		
11		O&M Labor Forecast	Forecast for existing employees labor costs	B	-	-	-	-	-	-	-	-	-	-	-	-		
12		O&M new FTEs	Forecast for new FTEs	P														
13		O&M IS Associate Program	Forecast for new IS Associate Program	P														
14		Two Factor Authentication	Refresh of two factor authentication infrastructure for remote and privileged user access	B	286	2	-	-	-									
15		Identity & Access Management	Single sign on capability with LAN ID for corporate systems Centralized identity and authentication management	B	786	1,002	1,180	38	(57)									
16		SAP Super User Provisioning	Implementation of Financial systems modules to enable provisioning of secure role profiles and access privileges	B	-	722	698	(399)	-									
17		SoCalGas Data Center Perimeter Rebuild	Data center perimeter rebuild including 20% of Information Security Intrusion Defense Systems (IDS)/Intrusion Prevention Systems (IPS) infrastructure project budget	B	5,613	1,502	1,116	(68)	-									
18		IS Infrastructure Network Zone Update	Replace obsolete racks and infrastructure in IS secure zones	B	1,517	3	-	-	-									
19		Private Field Network Expansion	Communication technology to support field area network devices	B	853	1,679	1,859	152	1,629									
20		Device Data Protection	Hard disk encryption	B	1	85	-	-	-									
21		Public Key Infrastructure (PKI)	PKI digital key encryption system to protect in transit and to authenticate devices, services, and applications	B	1,396	532	-	-	1,812									

2016 Risk Assessment Mitigation Phase  
SCG-03-WP  
Risk: Cyber Security (Capital)

Line No.	Mitigation	Project/Program	Project/Program Description	Recorded (Directs, 2015 \$000)						Forecast Range (Directs, 2015 \$000)						2017-2019 Low (Sum)	2017-2019 High (Sum)	Forecast Methodology
				Status	2011	2012	2013	2014	2015	2017 Low	2017 High	2018 Low	2018 High	2019 Low	2019 High			
22		Data Exfiltration	Data Loss Prevention - solution deployment to secure sensitive information egress for enterprise client end points, Mobile Data Terminals (MDTs), Customer Call Center (CCC)	B	-	-	-	-	312	-	-	-	-	-	-	-	-	
23		Malware Defenses	End Point Security - enterprise deployment of advanced, non-signature based, malware protection / prevention and analytics	B	-	-	-	-	2,672	-	-	-	-	-	-	-	-	
24		Email and Web Browser Protections	Solution deployment for internet email spam, phishing and malware filtering	B	592	3	-	-	-	-	-	-	-	-	-	-	-	
25		Security Small Capital Projects	Operations and reliability expenses associated with blanket work orders for replacement of failed IS production hardware and systems as necessary	B	193	209	53	-	-	-	-	-	-	-	-	-	-	
26		Converged Perimeter Systems		P						3,600	3,600	-	-	-	-	3,600	3,600	Base Year
27		Host Based Protection		P						2,500	2,500	-	-	-	-	2,500	2,500	Base Year
28		IS Zone Rebuild	Replace switches and Intrusion Prevention Systems (IPS) IS zone	P						950	950	-	-	-	-	950	950	Base Year
29		Web Applications and Database Firewalls	Security controls on servers. Deploy web application firewalls	P						-	-	2,250	2,250	-	-	2,250	2,250	Base Year
30		Enterprise Source Code Security	Proactive preventative application scanning, static analysis of source code before in house and/or third party software is released into production	P						-	-	1,300	1,300	-	-	1,300	1,300	Base Year
31		Wired Network Preventative Controls	Implement technical controls to authenticate substation devices before granting network access	P						-	-	3,500	3,500	-	-	3,500	3,500	Base Year
32		Multi Factor Authentication Refresh	single use token product or another similar solution	P						-	-	2,800	2,800	-	-	2,800	2,800	Base Year
33		My Account Multi Factor Authentication		P						-	-	1,800	1,800	-	-	1,800	1,800	Base Year
34		Protective Capability Infrastructure		P						-	3,000	-	3,600	10,000	16,000	10,000	22,600	Base Year
35	Protect Subtotal				11,236	5,740	4,907	(277)	6,368	7,050	10,050	11,650	15,250	10,000	16,000	28,700	41,300	
36	Detect	O&M GRC - Historical	Base business historical information	B	-	-	-	-	-	-	-	-	-	-	-	-	-	
37		O&M Non-Labor Forecast	Forecast for existing employees non-labor costs	B	-	-	-	-	-	-	-	-	-	-	-	-	-	
38		O&M Labor Forecast	Forecast for existing employees labor costs	B	-	-	-	-	-	-	-	-	-	-	-	-	-	
39		O&M new FTEs	Forecast for new FTEs	P						-	-	-	-	-	-	-	-	
40		O&M IS Associate Program	Forecast for new IS Associate Program	P						-	-	-	-	-	-	-	-	
41		Enterprise Logging Infrastructure	Enterprise log management system deployment	B	-	-	955	(44)	-	-	-	-	-	-	-	-	-	
42		Cyber Security Event Monitoring	Security Event/Incident Management (SEIM) consolidation into enterprise log management solution	B	1,516	(10)	-	-	-	-	-	-	-	-	-	-	-	
43		HTTPS Egress Decryption	Decrypt Secure Socket Layer (SSL) traffic at the perimeter to enable inspection	P						2,000	2,000	-	-	-	-	2,000	2,000	Base Year
44		Network Security Monitoring	Includes activities such as Packet Sled, Splunk, Threat Analytics	P						2,000	2,000	-	-	-	-	2,000	2,000	Base Year
45		Perimeter Tap Infrastructure Redesign	improved passive and by-pass tap technology	P						-	-	1,450	1,450	-	-	1,450	1,450	Base Year
46		Logging and monitoring infrastructure	Logging and monitoring infrastructure	P						-	2,000	-	2,000	4,000	5,450	4,000	9,450	Base Year
47	Detect Subtotal				1,516	(10)	955	(44)	-	4,000	6,000	1,450	3,450	4,000	5,450	9,450	14,900	

2016 Risk Assessment Mitigation Phase  
SCG-03-WP  
Risk: Cyber Security (Capital)

Line No.	Mitigation	Project/Program	Project/Program Description	Status	Recorded (Directs, 2015 \$000)					Forecast Range (Directs, 2015 \$000)						2017-2019 Low (Sum)	2017-2019 High (Sum)	Forecast Methodology
					2011	2012	2013	2014	2015	2017 Low	2017 High	2018 Low	2018 High	2019 Low	2019 High			
48	Respond	O&M GRC - Historical	Base business historical information	B	-	-	-	-	-	-	-	-	-	-	-	-	-	
49		O&M Non-Labor Forecast	Forecast for existing employees non-labor costs	B	-	-	-	-	-	-	-	-	-	-	-	-	-	
50		O&M Labor Forecast	Forecast for existing employees labor costs	B	-	-	-	-	-	-	-	-	-	-	-	-	-	
51		O&M new FTEs	Forecast for new FTEs	P						-	-	-	-	-	-	-	-	
52		O&M IS Associate Program	Forecast for new IS Associate Program	P						-	-	-	-	-	-	-	-	
53		Incident Response	Vendor solution for forensics infrastructure	B	977	2	-	445	-	-	-	-	-	-	-	-	-	
54		Enterprise Forensics	Rebuild of the forensics and ediscovery systems	B	1,394	115	-	-	-	-	-	-	-	-	-	-	-	
55		Security Orchestration	Automate key security triage tasks	P						2,000	2,000	-	-	-	-	2,000	2,000	Base Year
56		Incident Response Secure Collaboration	Deploy a communication and coordination platform that can be securely leveraged on the corporate network	P						-	-	2,000	2,000	-	-	2,000	2,000	Base Year
57		Incident Response Infrastructure		P						-	1,000	-	2,000	3,000	5,000	3,000	8,000	Base Year
58	Respond Subtotal				2,370	116	-	445	-	2,000	3,000	2,000	4,000	3,000	5,000	7,000	12,000	
59	Recover	O&M GRC - Historical	Base business historical information	B	-	-	-	-	-							-	-	
60		O&M Non-Labor Forecast	Forecast for existing employees non-labor costs	B	-	-	-	-	-							-	-	
61		O&M Labor Forecast	Forecast for existing employees labor costs	B	-	-	-	-	-							-	-	
62		O&M new FTEs	Forecast for new FTEs	P						-	-	-	-	-	-	-	-	
63		O&M IS Associate Program	Forecast for new IS Associate Program	P						-	-	-	-	-	-	-	-	
64		Security capability recovery infrastructure	Recovery infrastructure specific to security capability infrastructure	P						-	2,000	-	2,000	-	2,000	-	6,000	Base Year
65	Recover Subtotal				-	-	-	-	-	-	2,000	-	2,000	-	2,000	-	6,000	
66	TOTAL				\$ 15,122	\$ 5,847	\$ 6,240	\$ 104	\$ 6,368	\$ 13,050	\$ 23,550	\$ 15,100	\$ 27,200	\$ 17,000	\$ 30,950	\$ 45,150	\$ 81,700	

Notes:

- Baseline (B) and Proposed (P).
- Numbers in risk chapter tables may differ due to rounding.
- The purpose of Risk Assessment Mitigation Phase (RAMP) is not to request funding. Any funding requests will be made in the General Rate Case (GRC). The forecasts for mitigations are not for funding purposes, but are rather to provide a range for the future GRC filing. This range will be refined with supporting testimony in the GRC.