Application No.: A.23-05-010
Exhibit No.: SCE-04 Vol. 03
Witnesses: B. Barrios


(U 338-E)

# 2025 General Rate Case

## *Cybersecurity*

Before the

**Public Utilities Commission of the State of California**

Rosemead, California
May 12, 2023

# SCE-04 Vol. 03: Cybersecurity

## Table Of Contents

# SCE-04 Vol. 03: Cybersecurity

## Table Of Contents (Continued)

# SCE-04 Vol. 03: Cybersecurity

## Table Of Contents (Continued)

# I.
# INTRODUCTION

## A. Content and Organization of Volume

In this volume, SCE presents its Operations and Maintenance (O&M) expense forecast for the Test Year 2025 and 2023-2028 capital expenditures forecast for the Cybersecurity Business Planning Element (BPE). This includes cybersecurity activities and infrastructure for SCE's broader Grid Modernization effort detailed in Exhibit SCE-02, Vol. 06. SCE's forecasts reinforce the need for a cyber-safe environment, which is essential for our delivery of safer, more reliable, affordable, and clean power to our customers in a landscape where cyberattacks are becoming more sophisticated and more frequent. This volume also describes the scope of work, key drivers for the work, and legal requirements that impact the level of O&M and capital requested to support and successfully implement Cybersecurity activities.

## B. Summary of O&M and Capital Request

SCE's Test Year 2025 O&M forecast for Cybersecurity of $42 million, summarized in Figure I-1, is primarily driven by the risks identified in SCE's Risk Assessment and Mitigation Phase (RAMP) submission and the resources needed to address those risks. As the grid is modernized, there is a concurrent increase in the need to integrate information technology with operational technology and the associated costs are reflected in the forecast. This is discussed in greater detail in Section II.C.

SCE's Cybersecurity capital expenditures forecast is $760 million for 2023-2028, as summarized in Figure I-2. In addition to the continuation of ongoing cybersecurity capital programs, the capital forecast is driven by several new cyber-defense enhancements, including those driven by SCE's initiatives to build a more flexible and capable grid necessary to meet California's 2045 mandate and IT, OT, and third-party integration. These are discussed in greater detail below in Sections B.5.b, Basis of Forecast for "Cybersecurity Delivery," Section C.5.b, Basis of Forecast for "Grid Modernization Cybersecurity," and Section D.5.b, Basis of Forecast for "Software License and Maintenance."

***Figure I-1***
***Resiliency O&M***
*(Constant $000)*

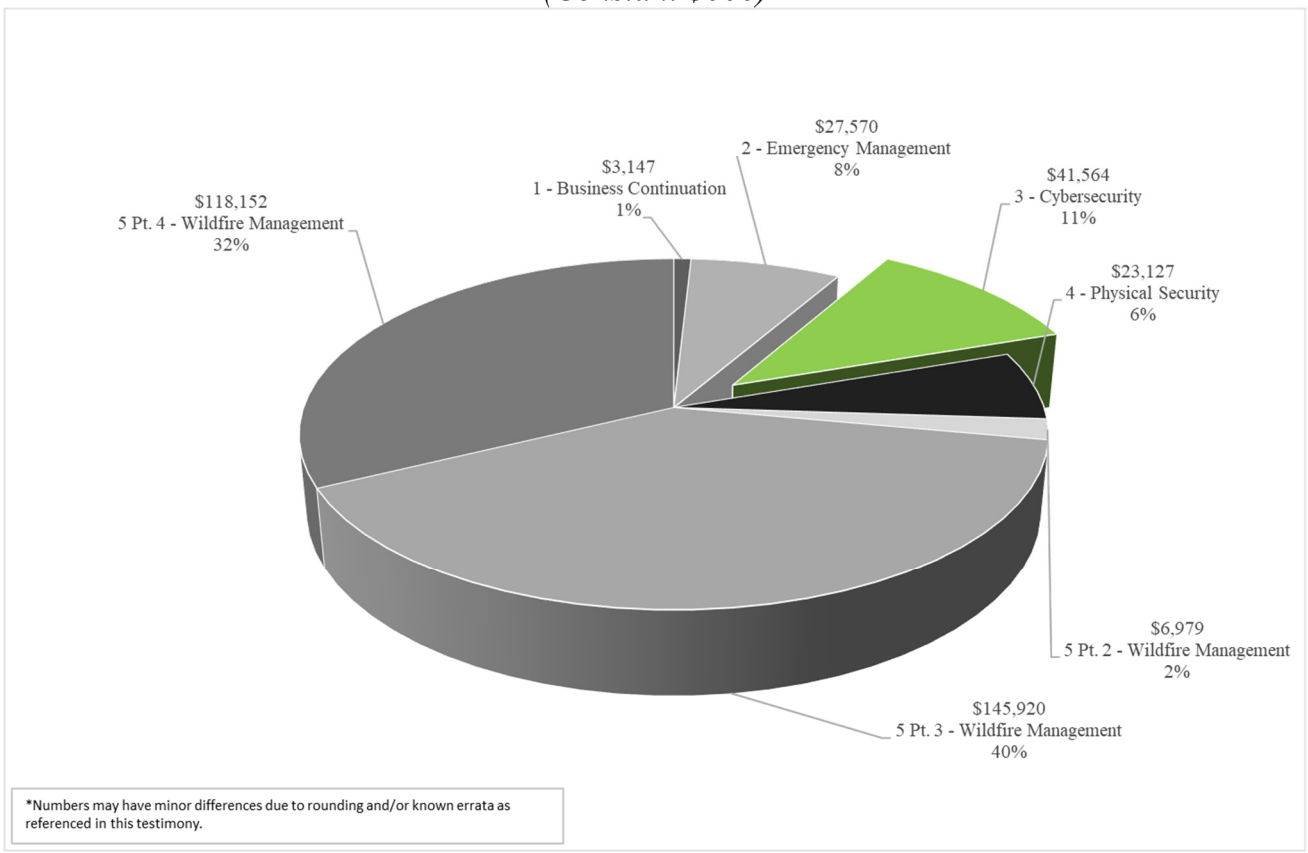
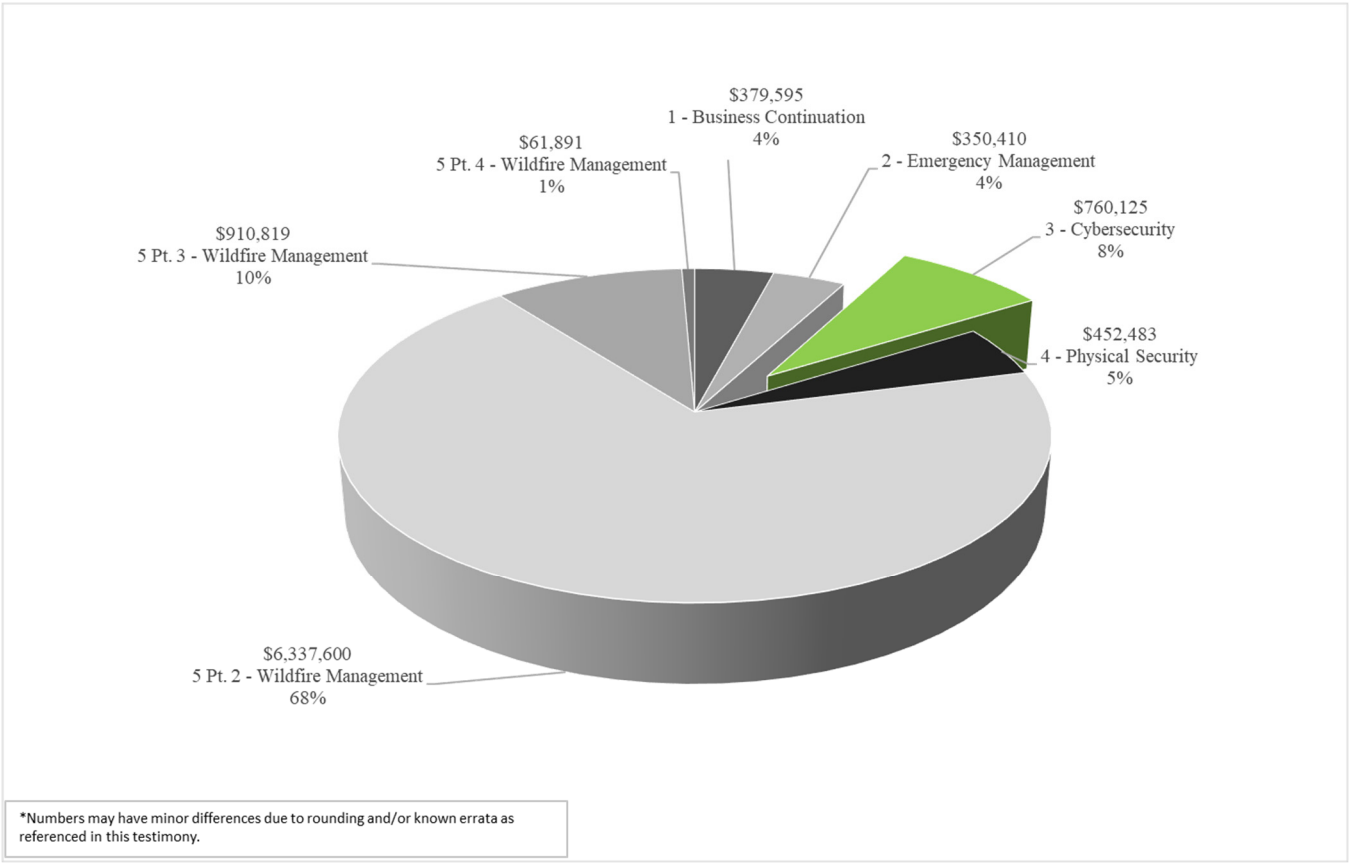


***Figure I-2***
***Resiliency Capital***
*(Nominal $000)*




*Numbers may have minor differences due to rounding and/or known errata as referenced in this testimony.

## II.

## CYBERSECURITY

### A. Overview

According to the FBI's 2021 Internet Crime Report,[1] global financial losses related to cybercrime increased 256% between 2018 and 2021, and reports of phishing, vishing, smishing, and pharming[2] increased 1,228% during this same period. The same report states that in 2021, the state of California had the highest cybercrime losses in the United States with more than $1.2 billion in victim losses, more than twice that of the second highest state (Texas). Unlike many businesses with IT assets, utilities have the added challenge of securing Operational Technology (OT) assets and infrastructure in a climate of rapidly increasing attacker capabilities. One study[3] found that 64% of utility professionals list sophisticated cyber-attacks as a top challenge. In 2022,[4] researchers analyzed 465 advisories covering 2,170 Common Vulnerabilities and Exposures (CVE) for OT and Industrial Control Systems (ICS), more than double that of 2020. Even more concerning, approximately half of these advisories could result in both loss of view and loss of control of the OT system. This growth represents a significant increase in both IT and OT risk.

Further, in the cybersecurity arena, our adversaries are many. Russia, for example, "is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis." China similarly has been assessed by the U.S. Intelligence Community, which states "China

---

1 Federal Bureau of Investigations (2021) "Federal Bureau of Investigation Internet Crime Report 2021" *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

2 Phishing, vishing, smishing, and pharming are terms used to describe cyber-attacks involving social engineering. The attackers perpetrate fraud by pretending to be a legitimate person or entity that the victim trusts. Examples include banks, online services, charitable or government organizations, etc. The attackers attempt to trick the victim into sharing confidential information such as account numbers, social security numbers, and login passwords. The variation in terminology reflects the technology used for the attack, such as email, phone call or voicemail, SMS text, or redirection of internet traffic to a malicious website.

3 Siemens, Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?, *available at* https://assets.siemens-energy.com/siemens/assets/api/uuid:c723efb9-847f-4a33-9afa-8a097d81ae19/siemens-cybersecurity.pdf.

4 Dragos, 2022 ICS OT Cybersecurity Year In Review, p. 58, (2022), *available at* https://www.dragos.com/year-in-review/.

almost certainly is capable of launching cyberattacks that could disrupt critical infrastructure services within the United States."[5]

There are many factors contributing to a need for continuously evolving cybersecurity practices within SCE. First and foremost is an ever-increasing role of technology and digitalization within both IT and Grid systems. Unfortunately, the same functionality that allows SCE to meet customer needs faster, more efficiently, and more reliably, can also be misused and abused. Be it theft of customer information for monetary gain, or disruption of power delivery related to geopolitical unrest, SCE represents an attractive target for cyber-attackers. Attacks on Ukraine's electrical system both prior to, and during, the Russian invasion have demonstrated how widespread disruption of power delivery can be used to destabilize and disrupt everyday life.

Another factor driving the need for continuous evolution of SCE's cybersecurity practices is the exponential growth of hacking tools, resources, and knowledge. Hacking services, where highly capable hackers charge a fee for their "services," allow virtually anyone to commission a cyber-attack against an individual or a business. The fees for these hacking services are relatively low; many attacks cost less than $1,000 and come with a money-back guarantee.[6] Beyond hacking services, availability of hacking tools and know-how is also growing exponentially. Libraries of CVEs provide detailed information about cyber vulnerabilities, and hacking tools and information are widely available at little or no cost.

One example of the devastating consequences that can come from the proliferation of hacking tools is the NotPetya[7] cyber-attacks in 2017. NotPetya used a hacking tool created by the U.S. National Security Agency (NSA) known as EternalBlue. The NSA lost control of EternalBlue during a data breach. This hacking tool played a major role in the NotPetya cyber-attack, one of the largest and most

---

[5] Office of the Director of National Intelligence, Worldwide Annual Threat Assessment of the US Intelligence Community (February 6, 2023), *available at* https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[6] Refer to WP SCE-04, Vol. 03, pp. 1 – 12. Paul Bischoff, "The Cost of Hiring a Hacker on the Dark Web: Report" (October 12, 2021), *available at* https://www.comparitech.com/blog/information-security/hiring-hacker-dark-web-report/.

[7] NotPetya is malicious software (malware) created by Russia and initially deployed against Ukraine as a cyberwar attack. Because this malware was designed to self-replicate indiscriminately, it quickly spread across the globe.

widespread cyber-attacks in history, and one which resulted in an estimated $10 billion in damages worldwide.[8]

Other examples of recent cyberattacks include the attacks against Colonial Pipeline and Kasaya. Both of these incidents involved ransomware in which the attackers installed malware that encrypted data on computers and servers, denying the company use of their systems until a ransom is paid to decrypt the data. In the case of Colonial Pipeline[9] in May of 2021, attackers first gained access to Colonial's network via an exposed password for a company Virtual Private Network (VPN) and stole 100 gigabytes of data. After stealing the data, the attackers used their access to install ransomware that spread throughout Colonial's network. To keep the ransomware from spreading further, Colonial shut down its gasoline pipeline system (which carries approximately 2,500,000 barrels daily) for a total of six days.[10] The impact of this attack was so great that President Biden declared an emergency and the company paid a ransom of $4.4 million in Bitcoin to get the decryption key from the attackers (the FBI was later able to recover $2.4 million of Bitcoin from the attackers).

In the case of the Kaseya ransomware attack,[11] also in 2021, the attackers exploited a zero-day vulnerability[12] in Kaseya's remote monitoring and management software. This software is used extensively by managed IT service providers (MSPs) worldwide to remotely manage computers, and it gave the attackers the elevated privileges necessary to install malware on the computers of some 1,500 businesses. The Kaseya attackers initially demanded $70 million in Bitcoin to provide the universal decryption key, but later reduced their demand to $50 million in Bitcoin. Following diplomatic talks

---

[8] Andy Greenberg, *The Untold Story of Not Petya, the Most Devastating Cyberattack in History,* WIRED, Aug. 22, 2018, *available at* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[9] Sean Michael Kerner, *Colonial Pipeline hack explained: Everything you need to know*, WHATIS.COM, Apr. 26, 2022, *available at* https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[10] Nicole Perlroth, David E. Sanger, Clifford Krauss, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline,* NEW YORK TIMES, May 13, 2021, *available at* https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

[11] Clare Duffy, *A massive ransomware attack hit hundreds of businesses. Here's what we know*, CNN BUSINESS, July 7, 2021, *available at* https://www.cnn.com/2021/07/06/tech/kaseya-ransomware-what-we-know/index.html.

[12] *See* Josh Fruhlinger, *Zero days explained: How unknown vulnerabilities become gateways for attackers,* CSO, Apr. 12, 2021, *available at* https://www.csoonline.com/article/3284084/zero-days-explained-how-unknown-vulnerabilities-become-gateways-for-attackers.html

between the US and Russian governments, the attacker's servers were quickly taken down and the decryption key was provided to Kaseya through an un-named third-party.

Both the Colonial Pipeline and Kaseya attacks reveal the impact-amplification potential of cyberattacks across a supply chain ecosystem. For Colonial Pipeline, the cyberattack shutdown only one company, but that company supplies gasoline, diesel, jet fuel, and heating oil to most of the Eastern United States. The Kaseya cyberattack demonstrates how one vulnerability in one software product can have devastating impacts on hundreds or thousands of organizations and businesses. A successful attack to a company's supply chain ecosystem can be devastating, so SCE must be prepared, vigilant, and resilient through our own cybersecurity programs.

One final example involved a long-term attack campaign against the software SolarWinds that resulted in approximately 18,000 users, including large corporations and the U.S. Government, being vulnerable to a variety of cyberattacks. The attack campaign also allowed the adversaries access into protected information systems.[13] According to a report from IronNet, the average cost per respondent was estimated to be 11% of their annual revenue, or $12 million per company.[14]

There is no shortage of examples to demonstrate the potential impact cyber-attacks can have on an organization. The examples above are just a small sampling. The reality is that the economics of cyber-attacks make it very attractive for those with the knowhow and tools to set their sights on an organization like SCE. From simple cyber criminals seeking a quick financial gain via ransomware, to sophisticated nation-states actors who desire a persistent capability to disrupt power delivery to key infrastructure, SCE is a tantalizing target for cyber-attackers. SCE's cybersecurity team must protect an increasing variety of systems, services, and technologies, which means we must continue to invest in people, software, tools, processes, and knowhow to stay ahead of attackers.

While cyber threats and attacks are increasing, SCE is also facing an unprecedented change to the underlying construction of our grid infrastructure and grid operating principles. California's Senate Bill 100 mandates 100 percent renewable energy by 2045. It also includes a requirement for 60 percent

---

[13] Reuters Staff, *SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president*, REUTERS, Feb. 14, 2021, *available at* https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-microsoft-president-idUSKBN2AF03R.

[14] Veronica Combs, *Cybersecurity study: SolarWinds attack cost affected companies an average of $12 million*, TECHREPUBLIC, June 28, 2021, *available at* https://www.techrepublic.com/article/cybersecurity-study-solarwinds-attack-cost-affected-companies-an-average-of-12-million/.

of all energy consumed in the state to come from renewable sources by 2030. New technology and exponentially more data consumption are required to accomplish these monumental objectives. With these new technologies and new data connections, some of which will be from interfaces with third parties, new and unique cybersecurity architectures and controls must be designed, tested, and implemented to ensure the security of our critical grid infrastructure. This effort goes well beyond the regular activities and incremental progression that would occur within a typical GRC request. It is imperative that the cybersecurity budget increases forecasted in this testimony reflect the effort and expenditures that will be necessary to meet the California legislature's mandate with cyber-protected technologies and systems.

**1. Compliance Requirements**

The Commission required that SCE "include its own forecast and the Commission's adopted forecast from the previous GRC alongside historical costs, and brief explanations detailing any changes in the scope of a category."[15] A summary is provided below and within the respective testimony for each GRC activity.

In the 2018 GRC, SCE supported the recommendation for establishing a separate proceeding to address how sensitive cyber-related information should be shared during a GRC.[16] The Commission agreed with SCE, stating, "further review of how to address cyber-related information would be appropriate in another forum."[17] While there is no corresponding compliance requirement or proceeding opened to-date, SCE remains supportive of collaborating with parties to formally establish standard processes and to assess the manner in which sensitive cybersecurity information may be shared with intervenors and Commission staff.

Similar to previous proceedings, SCE's cybersecurity efforts include protecting the electric grid, which has been designated by the Department of Homeland Security (DHS) as critical infrastructure.[18] Therefore, a secure process for disclosing detailed tactics, techniques, and procedures to

---

[15] D.15-11-021, p. 224.

[16] A.16-09-001, Exhibit SCE-20, Vol. 01, pp. 40-42.

[17] D.19-05-020, p. 154.

[18] DHS identifies 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The U.S. Energy Sector is defined as one of these Critical Infrastructure sectors, Cybersecurity & (*Continued*)

stakeholders in this proceeding is also needed to help ensure the protection of this sensitive data. In this rate case, we have made every effort possible to disclose information that will help substantiate our forecast increases without compromising security. However, to help the Commission access other information necessary to answer specific questions regarding the cyber security risks, mitigations, and cost forecasts, SCE remains amenable to provide an in-person briefing or to engage in other appropriate methods (such as virtual sharing platforms or a reading room)[19] to securely share additional details that we cannot disclose in this testimony for reasons of safeguarding the integrity of the grid and protecting public safety.

**2. Risk factors, Safety, Reliability and Connection with RAMP**

Cybersecurity was identified as one of SCE's top risks and was included in the 2022 Risk Assessment and Mitigation Phase (RAMP) report. The section below summarizes the risk factors, controls and mitigations discussed in SCE's RAMP submission as they inform SCE's O&M and Capital forecasts presented herein.

To define and evaluate the risk of cyberattack within SCE's environment, SCE constructed a cyberattack risk bowtie. Each component of the bowtie represents a critical data point in evaluating this risk. SCE's RAMP Report explains these components in detail and identifies several options to mitigate the risk (including Risk Spend Efficiency), all of which inform the forecasts in this volume. Figure II-3 shows the cyberattack Risk Bowtie.

Cybersecurity threats continue to grow in number, sophistication, and complexity, with increasingly severe impacts. SCE's cybersecurity strategy must continuously evolve and adapt to keep pace with these ever-evolving threats. Like prior GRC filings, SCE organizes its cybersecurity defense into five program areas outlined in detail below. Each program area supports SCE's strategic effort to mitigate the risk of cyberattacks.

During the 2022 RAMP development process, SCE quantified the estimated rate of occurrence, risk outcome, and consequence reduction for each program area. The risk analysis identified three key drivers: (1) External Actors, (2) Insider Threats, and (3) Supply Chain attacks. These drivers are associated with Outcomes that each have consequences with safety, reliability, and/or financial

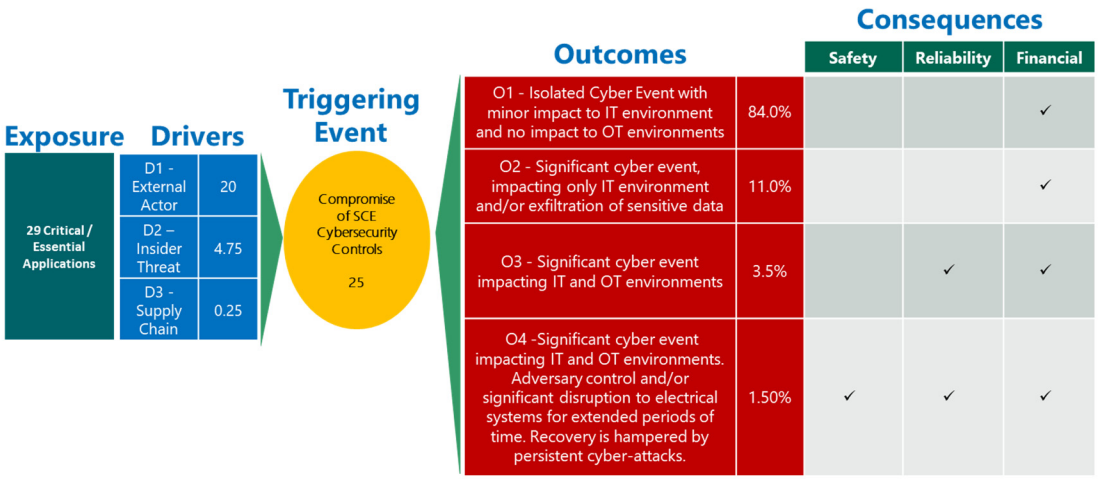
---

Infrastructure Security Agency, Critical Infrastructure Sectors, *available at* https://www.dhs.gov/critical-infrastructure-sectors.

[19] Refer to WP SCE-04, Vol. 03, pp. 13 – 15 "Potential Use of Virtual Sharing Platforms."

dimensions. The impacts of those Outcomes range in severity from outcome 1 (an isolated attack with minor impact on IT systems and purely financial impact) to outcome 4 (a significant attack with safety, reliability, and financial impact) as detailed in the RAMP Report.

***Figure II-3***
***SCE 2022 RAMP Cyberattack Bowtie***




The following mitigation programs were evaluated and included as part of SCE's 2022 RAMP Report: (1) Perimeter Defense, (2) Interior Defense, (3) Data Protection, and (4) Supervisory Control and Data Acquisition (SCADA) Cybersecurity. Table II-1 shows the RAMP Control/Mitigation (Programs) related to cybersecurity and risk mitigations.

*Table II-1*
*RAMP Controls/Mitigation and Risks Addressed*

| RAMP Risk Addressed | GRC Activity | 2022 RAMP ID | 2022 RAMP Control/Mitigation Name |
|---|---|---|---|
| Cyber Attack | Cyber Software License and Maintenance | C1 | Perimeter Defense |
| | Cyber Software License and Maintenance | C2 | Interior Protection |
| | Cyber Software License and Maintenance | C3 | Data Protection |
| | Cyber Software License and Maintenance | C4 | SCADA Cybersecurity |
| | Cyber Software License and Maintenance | C5 | Grid Modernization Cybersecurity |
| | Cybersecurity Delivery and IT Compliance | C1 | Perimeter Defense |
| | Cybersecurity Delivery and IT Compliance | C2 | Interior Protection |
| | Cybersecurity Delivery and IT Compliance | C3 | Data Protection |
| | Cybersecurity Delivery and IT Compliance | C4 | SCADA Cybersecurity |
| | Cybersecurity Delivery and IT Compliance | C5 | Grid Modernization Cybersecurity |
| | Grid Mod Cybersecurity | C5 | Grid Modernization Cybersecurity |

As further discussed in SCE's RAMP Report, cybersecurity risks facing SCE's grid operating systems continue to grow in volume, severity, and complexity. SCE analyzed these risks and created tiers of risk mitigation, which will be discussed further below. SCE defends against the growing and persistent threat of cyber-attacks by implementing enhanced capabilities referenced in our cybersecurity capital programs, updating cyber defense software and related resources pursuant to multiple software licenses, maintenance, and support agreements, and dedicating sufficient labor and non-labor resources to support ongoing and evolving cybersecurity programs.

**a) Safety Policy Division Comments**

Below are the observations and recommendations from the Commission's Safety Policy Division's (SPD) review of SCE's 2022 RAMP report:

**Observation #1:** For the Cybersecurity risk chapter, SCE's risk bowtie could be improved to more clearly explain how the potential risk event could be brought to bear; such improvement would bring the cybersecurity risk bowtie closer to meeting expectations and dynamic changes in means and methods. As submitted, the SCE risk bowtie equates subcategories of exposure (i.e., insider threat, supply chain procurement malware) with risk drivers. This has the effect of misidentifying a given trigger event that brings the risk event to be.

**SCE Response:** SCE believes that Insider Threat, External Actor, and Supply Chain (the three key identified risk drivers) are better represented as Risk Drivers, rather than as subcategories of exposure. For example, an Insider Threat risk driver can utilize the supply chain as an attack vector. The attack vector is the method (or source) of the attack used by the bad actor against the

target. This enables the trigger event to be abstracted as a compromise of system security controls without listing all the possible combinations of Risk Drivers and attack vectors.

**Observation #2:** As in the 2018 RAMP filing, SCE's 2022 Analysis Scope of Work and Limitations for the cybersecurity risk RAMP chapter provides a disclaimer noting that SCE's analysis does not speak to resulting significant secondary impacts involving a cyber-attack. As part of the risk and consequence analysis, SCE should attempt to quantify worst-case scenarios and secondary impacts developed via their risk assessments, work with government agencies (e.g., U.S. Department of Homeland Security's Assessment of Electricity Disruption Incident Response Capabilities) and apply the result of simulations and tabletop exercises such as those performed with GridEx.

**SCE Response:** SCE did consider secondary impacts from a cybersecurity event. During the development of the RAMP testimony, Cybersecurity worked directly with other SCE organizations and advisors on risks, such as Battery Energy Storage Systems (BESS) and Public Safety Power Shutoff (PSPS) to evaluate which of their outcomes could be triggered or amplified by a cybersecurity event. We also used this data to estimate how consequences for those environments could be increased by a cybersecurity event as a secondary impact. The safety, reliability, and financial inputs from those organizations were used to calculate the Cybersecurity impacts and likelihood of a cybersecurity event was used as a cross-cutting factor that applied to those risks. SCE participated as both a planner and player in GridEx VI and continues to apply the learnings from this and other national exercise participations. SCE is a partner in multiple projects with the Department of Energy, including its National Laboratories, and with the Department of Homeland Security to maintain active relationships, information sharing activities and pilot national security initiatives. In addition, SCE was a participant of the CPUC-sponsored California Energy Systems for the 21st Century which explored machine-to-machine automated threat responses in a major cyber-attack.

**Observation #3:** As with other risks, SCE omitted RSE values for Controls, omitting discussion of 2018 RAMP control descriptions, including one pertaining to Federal compliance obligations. As mentioned in earlier chapters, Decision 21-11-009 requires the calculation of RSEs for risk mitigation, including those previously categorized as controls associated with regulatory compliance obligations.

**SCE Response:** SCE disagrees with SPD and TURN's interpretation of D.21-11-009 and the need to provide risk spend efficiencies (RSEs) for compliance-based programs. However, as noted in SCE-01 Vol. 02, SCE has provided RSE values for the compliance programs

discussed in RAMP. As SCE did not discuss NERC CIP cyber work in the RAMP filing, SCE did not provide an RSE for that work in this GRC.

**Observation #4:** SCE does not adequately explain or justify why the utility proposes a four-year mitigation (risk containment) plan that totals $531.2 million, or about $132.8 million per year to continue five controls addressing three risk tranches. SCE's proposed spending amount represents a sizeable increase over prior spending levels for this risk category, with a total 2018 RAMP budget of just $477.4 million covering a six-year period, amounting to a past annual spend of only $79.6 million. One indicator of SCE's rising costs for its Cybersecurity is the overhead cost, or what's referred to in the RAMP as O&M. SCE's 2018 RAMP had O&M costs of $21.5 million in annual spending compared to SCE's 2022 RAMP O&M costs of $34.8 million per year. O&M costs as a share of overall Cybersecurity program costs increased slightly from 25 percent in the 2018 RAMP to 26 percent in the 2022 RAMP. It's worth noting that SCE's O&M for this risk is in the high range, with typical IOU O&M program costs tending to account for closer to 10 percent of overall program costs.

SCE indicates that its existing and planned approach to Cybersecurity appears to be adequate for the cyber threats that exist today. However, SCE anticipates a steady growth in cybercrime and increased capability and sophistication of malicious cyber actors. As a result, SCE proposes increased spending to evolve and expand its cybersecurity defenses. SCE should better substantiate the need for increased spending.

**SCE Response:** The total effort and cost needed to secure SCE's infrastructure and assets against external and internal cybersecurity threats correlates to 1) the total amount of digital assets presents within SCE's operations, and 2) cyber threat capabilities and activities. In other words, SCE's cybersecurity control programs must scale in relation to the increased cyber risk associated with a larger attack surface of both aging and new technologies, as well as increased cyber-attacker knowledge, capabilities, and tools. These risks are not static. Thousands of new vulnerabilities are identified each year,[20] which creates a never-ending requirement to update, patch, or mitigate these vulnerabilities with external controls. As new technologies are integrated and networked into field environments, such as transmission and distribution substations, they must be protected and monitored to ensure they are not being hacked for destructive purposes, or their network connections leveraged by an attacker to gain access to SCE's broader IT and OT networks. Each year, more and more technology is implemented to

[20] *See* Section 2.A. Overview Section for specific statistics re: year over year increase of cyberattacks.

improve services, to automate processes that were previously performed manually, and to optimize the services and value we deliver to our clients. California's 2045 mandate for 100% renewable energy is, and will continue to, drive unprecedented use of technology (and cybersecurity protections) to integrate and safely manage distributed energy generation and storage. Additionally, within IT's portfolio,[21] between the GRC filing for 2021 and this GRC filing for 2025, SCE's:

- Total number of on-premises licenses, Software as a Service (SaaS) and Cloud subscriptions has grown by 52 percent;
- Number of IT interfaces has increased by 67 percent;
- Number of midrange servers has increased 19 percent, and the total number of appliances has increased by 150 percent; and
- Number of cellular devices has increased 67 percent.

Lastly, observation #4 suggests that O&M is merely overhead. In practice, however, O&M represents the ongoing activities necessary to protect, monitor, and actively defend a constantly growing and increasingly complex baseline of technical capabilities against cyber-attacks, as detailed in the Overview section of this testimony. In SCE's experience, the aforementioned "10 percent of overall program costs" allocation for O&M that the SPD cites as "typical IOU O&M program costs" only supports a "run and maintain" approach of existing systems, without factoring in improvements or growth of capabilities necessary to adapt to increasing cybersecurity threats and adversaries.

**b) Risk Modeling Discussion**

There were no substantive updates from the RAMP filing to our Cyber risk models. Within the GRC, we looked to revisit modeling the risk of cyber-attacks, however, we continued to experience challenges as mentioned in our RAMP filing. As stated in our RAMP filing, in examining asset-based risks, such as the risk of damage to distribution overhead conductor from unmanaged vegetation growth, we can evaluate actual failure rates and equipment conditions, and leverage decades worth of utility data and information related to the performance of an asset. In contrast, cybersecurity does not have a similar breadth of data that we can draw upon when analyzing the risks. In light of the lack of cybersecurity data and information that is publicly shared, the Risk Spend Efficiency (RSE) parameters in RAMP do not meaningfully capture the manner in which cybersecurity

[21] *See* SCE-06, Vol. 01 Enterprise Technology for 2025 GRC statistics.

risk is assessed and mitigated based on the defense-in-depth model.[22] Additionally, unlike most asset-based risks, cyber-attacks are ever-evolving; what we know today may not be applicable to where the threat goes tomorrow, a year from now, or five years from now. As a result, SCE has to leverage whatever limited industry data is available, develop prudent assumptions, and consult with industry experts to validate our approach to this risk evaluation. SCE recognizes that not capturing indirect, or secondary impacts from risk events can underestimate the potential magnitude of a risk. To alleviate this concern, SCE participated as both a planner and player in GridEx VI and continues to apply the learnings from this and other national exercise participations. SCE is a partner in multiple projects with the Department of Energy including its National Laboratories, and with the Department of Homeland Security to maintain active relationships, information sharing activities and pilot national security initiatives. In addition, SCE was a participant of the CPUC-sponsored California Energy Systems for the 21st Century which explored machine-to-machine automated threat responses in a major cyber-attack.

In addition, the level of detail and disclosure that SCE can provide in RAMP and in the GRC with regard to cybersecurity needs, capabilities, and gaps must be balanced with the need to keep such critical information confidential and prevent it from falling into the hands of an ill-intended actor who may use the information for harmful purposes.[23] SCE outlined the issue in its RAMP Report, and offered additional solutions for the Commission to obtain further cybersecurity information in a reasonably secure manner. For example, SCE stated the following:

> The detailed analysis that we performed internally around cybersecurity has informed the discussion we present in this chapter. However, SCE must necessarily safeguard this critical information. SCE's cybersecurity efforts include protecting the electric grid, which has been designated by the Department of Homeland Security (DHS) as critical infrastructure. [citation omitted] Therefore, a secure process for disclosing detailed tactics, techniques, and procedures to stakeholders to this proceeding is needed to help ensure its protection.

---

[22] Please refer to Mr. LeMoine's policy testimony in SCE-01, Vol. 02.

[23] SCE did include in its RAMP an explanation of the increasing level of threats of cyberattacks, including citation to prominent third-party sources. *See, e.g.*, SCE RAMP, Chap. 7, pp. 7-8. SCE's RAMP also showed that cyber-attackers are increasingly targeting electric utilities, with citation to governmental authorities and third-party experts. *See* SCE RAMP, Chap. 7, pp. 9-10.

> To help the Commission access the information necessary to answer **specific questions regarding the cybersecurity risks, mitigations, and cost forecasts**, SCE can provide an in-person briefing or engage in other appropriate methods to share additional detail that we cannot disclose in this Report for reasons of safeguarding the integrity of the grid and protecting public safety. One such method could be utilization of virtual sharing platforms. SCE provides a detailed workpaper that addresses and explains potential use of virtual sharing platforms in the specific context of the Commission's review of the RAMP Cyber Attack chapter.[24]

SCE did not receive any follow-up from SPD, or any other arm of the Commission regarding SCE's offers to provide additional cybersecurity information (specifically including cost forecasts) in a prudently secure manner.

**c) <u>RAMP Integration</u>**

As part of SCE's 2022 RAMP process, and similar to our 2018 RAMP approach, we examined three broad categories of cyber-attackers / drivers. The first category is attacks that originate outside of SCE's organization, infrastructure, and supply chains. These are known as External Attacks. The second category represents those associated with individuals and systems that are authorized, to a greater or lesser extent, to use SCE assets and systems. Be it accidental actions of carelessness or human error, or intentional misuse or abuse of access entrusted by SCE, Insider Threats pose a serious risk to all organizations including SCE. The final cyber-attack driver category examined during RAMP was Supply Chain. All large organizations operate within a supply chain consisting of suppliers, consumers, customers, and support entities. To maximize efficiencies that bring better, more affordable, and more reliable services to SCE customers, various levels of system and process integration exist between SCE and key suppliers. Cyber-attackers who may not succeed in attacking SCE directly may find alternate avenues into SCE systems through our suppliers.

Although the RAMP drivers were similar to prior years, the rate of attack occurrence was significantly higher in the 2022 RAMP than in our 2018 RAMP filing. This increase in estimated annual attacks reflects the reality that cyberattacks are growing exponentially. Not only are the number of attacks growing each year, but the diversity of attacks and the tools and resources used by attackers are also expanding rapidly. As such, our RAMP analysis reflects a greater number of attacks annually.

---

[24] SCE RAMP Report, Chap. 7, p. 6 (emphasis added).

In 2022, SCE slightly revised the cyber-attack outcomes definitions over those used in our 2018 RAMP filing. Moving from a five-point scale in 2018 to a four-point scale in 2022, SCE changed the outcome descriptions to be more inclusive of IT and OT system impacts, and to differentiate outcomes with financial and reliability consequences from outcomes with safety and reliability consequences.

Another improvement change in our 2022 RAMP process is the methodology used to estimate mitigation control effectiveness. The team examined the elements of each mitigation control program and estimated how effective each program would likely be against each attack driver. The result represents the percentage of attacks our subject matter experts believe could be thwarted with each mitigation control both individually, and collectively, across all controls. This approach proved helpful in determining mitigation effectiveness and Risk Spend Efficiency (RSE) scores.

SCE's 2022 RAMP evaluation represents our most complete consideration of risk mitigation effectiveness and spending efficiency to date. As such, we are leveraging it again for this GRC filing.

### 3. Regulatory Drivers Influencing SCE's Request

SCE's defense-in-depth[25] strategy is responsive not only to the need to secure our infrastructure; it is also responsive to the regulatory and policy signals coming from our State and Federal government partners. The National Cybersecurity Strategy, developed by leaders across the federal government, reinforces this concept by placing responsibility for managing cyber risk to the Nation's critical infrastructure on both the private sector and the Federal Government. In recognition of this shared priority, SCE's government partners may choose to collaborate with the industry to develop guidelines or best practices, voluntary programs, regulatory mandates, or a combination of the above. SCE, in turn, seeks to meaningfully leverage these voluntary and mandatory resources to inform and prioritize our cybersecurity efforts. Many of these mandatory standards represent a beneficial floor for cybersecurity practices; however, the voluntary frameworks, programs, and other partnerships can equally improve SCE's cybersecurity posture. Where we exceed minimum standards, we do so as we reasonably believe the risk-reduction benefit for our customers justifies the additional cost.

---

[25] "Defense-in-Depth" refers to a layered or redundant approach to security in which systems or information are protected by multiple independent and diverse layers of defensive technology, thus reducing the likelihood of successful attack. These layered defenses also afford cybersecurity analysts greater opportunity to detect and thwart attacks before the attackers can achieve their objectives.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard represents one of these key mandatory drivers for SCE's security strategy and investments. The NERC CIP standards mandate certain cybersecurity controls and processes based on how critical an asset or system is to the reliable operation of the bulk power system. In addition to developing these standards, NERC also conducts routine audits to verify compliance with the standards, and violations for non-compliance often result in fines, up to $1.5 million per violation per day.

Beyond the current mandatory standards, a variety of voluntary but encouraged frameworks have been developed by the industry and/or the government and help inform SCE's security investments. Examples for these include the National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF), the Department of Energy's Cybersecurity Capability Maturity Model (C2M2), and the Cybersecurity and Infrastructure Security Agency's (CISA) "Shields Up" guidance,[26] which outlined controls strongly encouraged by CISA in response to the heightened risk to critical infrastructure as a result of the conflict between Russia and Ukraine. The importance of these investments, particularly in light of the Russia/Ukraine conflict, was reinforced in a March 2022 letter from President Biden to State Governors, where the President called on states and critical infrastructure owners and operators to take appropriate and urgent steps to protect critical infrastructure. SCE is also closely monitoring a variety of emerging mandatory standards that are at various stages of development and which would require additional investment. Some examples of this include the Department of Defense's Cybersecurity Maturity Model Certification (CMMC),[27] CISA's sector-specific Baseline Performance Goals,[28] various reporting requirements proposed by CISA and the Securities and Exchange Commission (SEC),[29] and the potential distribution-level cybersecurity requirements proposed by the White House and Congress. Due to the wide potential range of compliance scopes, and the wide range of associated costs those would necessitate, these speculative investments are not included in this filing.

---

[26] Cybersecurity & Infrastructure Security Agency, Shield Up, *available at* https://www.cisa.gov/shields-up.

[27] United States of America, Department of Defense, Chief Information Officer, CMMC Model, *available at* https://dodcio.defense.gov/CMMC/Model/.

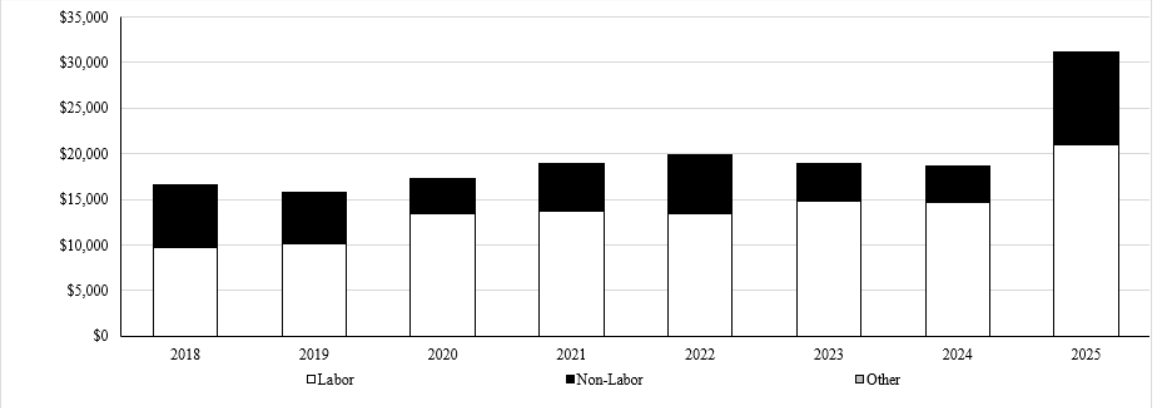
[28] Cybersecurity & Infrastructure Security Agency, Cybersecurity Cross Sector Cybersecurity Performance Goals, *available at* https://www.cisa.gov/cpgs.

[29] Examples include: Cybersecurity & Infrastructure Security Agency, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), *available at* https://www.cisa.gov/circia.

## B. Cybersecurity Delivery

Figure II-4 Cybersecurity Delivery shows 2018-2022 recorded costs and Test Year 2025 forecast for the Cybersecurity Delivery activity.

***Figure II-4***
***Cybersecurity Delivery O&M Expenses***[30]
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

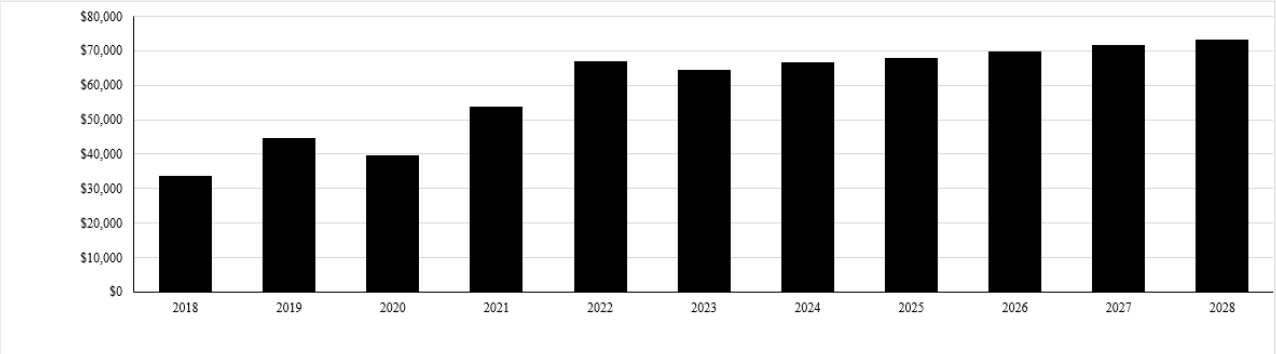



| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $9,752 | $10,160 | $13,387 | $13,669 | $13,416 | $14,756 | $14,631 | $21,037 |
| *Non-Labor* | $6,859 | $5,641 | $3,842 | $5,212 | $6,517 | $4,151 | $3,986 | $10,090 |
| *Other* | | | | | | | | |
| Total Expenses | **$16,611** | **$15,801** | **$17,229** | **$18,881** | **$19,933** | **$18,907** | **$18,616** | **$31,127** |

Figure II-5 shows 2018-2022 recorded expenditures and the 2023-2028 capital forecast for the Cybersecurity Delivery activity.

[30] Refer to WP SCE-04, Vol. 03, pp. 16 – 28, Cybersecurity Delivery – Standard Workpapers.

***Figure II-5***
***Cybersecurity Delivery Capital Expenditures***[31]
***2018-2022 Recorded / 2023-2028 Forecast***
*(Nominal $000)*




| | Recorded | | | | | Forecast | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 |
| Cybersecurity Delivery and IT Compli: | $33,485 | $44,701 | $39,453 | $53,663 | $66,833 | $64,429 | $66,605 | $67,905 | $69,737 | $71,457 | $73,220 |
| **Totals** | **$33,485** | **$44,701** | **$39,453** | **$53,663** | **$66,833** | **$64,429** | **$66,605** | **$67,905** | **$69,737** | **$71,457** | **$73,220** |

## 1. Project or Program Description

As cybersecurity threats significantly increase in volume and complexity year over year, SCE must continually adapt its defense strategies. SCE's Defense-in-Depth approach to cybersecurity leverages multiple layers of protection to prevent unauthorized access and control of our systems. The National Institute of Standards and Technology (NIST), which is an arm of the U.S. Department of Commerce, has promulgated and utilized the following definition for defense-in-depth: "The application of **multiple countermeasures in a layered or stepwise manner to achieve security objectives**. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure **that attacks missed by one technology are caught by another**." Thus, the different cyber security mitigations do not just interconnect; they cover for each other so that, in NIST's words, "attacks missed by one technology are caught by another." (emphasis added)[32]

Moreover, the Cybersecurity and Infrastructure Security Agency (CISA), part of the Department of Homeland Security (DHS), has published guidance recommending the use of defense-in-depth for organizations with OT environments, because it "increases the difficulty to access the control

[31] Refer to WP SCE-04, Vol. 03, pp. 16 – 28, Cybersecurity Delivery – Standard Workpapers.

[32] Keith Stouffer, et al., National Institute of Standards and Technology, NISTIR 8183 Cybersecurity Framework Manufacturing Profile, (Sep. 2017), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

system."[33] CISA's predecessor organization, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) also recommended the use of a defense-in-depth strategy for organizations that are considered critical infrastructure, such as electric utilities.[34] Additionally, the National Security Agency (NSA) within the U.S. Department of Defense has published a technical report containing guidance on network architecture using defense-in-depth, or "multiple layers of defense", to help secure environments.[35] Defense-in-depth is also included in the U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2) under the Cybersecurity Architecture domain.[36] This domain is assessed to create a maturity indicator level (MIL) based on an organization's advancement towards incorporating cybersecurity into their IT and OT architecture. SCE uses the C2M2 as a data point to track progress for overall IT and OT cybersecurity.

SCE's cybersecurity defense strategy is divided into five program areas: (1) Perimeter Defense, (2) Interior Defense, (3) Data Protection, (4) SCADA Cybersecurity; and (5) North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Compliance. Each of these require significant investments in O&M and in Capital. In addition to the ongoing cybersecurity programs, SCE's O&M and Capital forecast increases are driven by mitigation of risks to new and emerging threats, a greater need for government collaboration, the growing number of potential non-NERC compliance requirements, and addressing Cybersecurity implications due to the increased connectivity of Grid/IT technologies. These are discussed in greater detail in the forecast analysis sections below.

SCE's Cybersecurity Delivery organization works to enable our organization to realize the benefits and efficiencies of technology safely, avoiding excessive risk to the confidentiality,

---

[33] Cybersecurity & Infrastructure Security Agency, Layering Network Security Through Segmentation, (Jan. 2022), *available at* https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf.

[34] U.S. Dept. of Homeland Security, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, (2016), *available at* https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[35] U.S. National Security Agency, Network Infrastructure Security Guide (June 2022), *available at* https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF.

[36] U.S. Dept. of Energy, Cybersecurity Capability Maturity Model (C2M2), (Ver. 2.0, July 2021), *available at* https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf.

integrity, and availability of these systems and the critical data they contain. The SCE Cybersecurity group is organized into three primary areas: (1) Cybersecurity Engineering, Risk, and Governance, (2) Cybersecurity Architecture Technology and Operations, and (3) National Security Policy Advocacy and Cybersecurity Awareness Program

**1) Cybersecurity Engineering, Risk, and Governance (CybERG*)***

This group is responsible for establishing and maintaining cybersecurity policies, standards, and procedures. It is also responsible for cybersecurity lifecycle risk management of systems and assets including pre-production system testing and ongoing risk assessments and cybersecurity engineering consultation to both IT and OT stakeholders. The CybERG team plays a critical role in enabling the grid transformation to securely enable renewable energy technologies necessary for SCE's Pathway 2045 strategic plan. These enabling technologies must be secured from the growing list of sophisticated cybersecurity adversaries, many of whom are supported by Nation States, who seek to disrupt California's economy. Additionally, CybERG continuously monitors and assesses supply chain risk management controls to protect SCE from cyberattacks that involve our supply chain.

The Cybersecurity Engineering team works with business stakeholders to ensure Interior Defense, Perimeter Defense, and Data Protections are integrated into all technology projects and procedures across the enterprise. Additionally, the Engineering team works with the Cybersecurity Risk team to create compensating controls and/or remediation plans for potential risks and vulnerabilities that have been assessed.

SCE's Cybersecurity Risk team identifies areas where the confidentiality, integrity, or availability of SCE's systems and/or data may be at risk. This includes third-party risks to SCE's data or systems. Risk assessments allow SCE to make risk informed technology decisions by providing qualification and quantification of cyber risk impact and likelihood. Cybersecurity risk, vulnerabilities, and standards deviations found in the assessment process are given to the Cybersecurity Engineering team to develop compensating controls or remediation plans.

The Governance group works closely with the Cybersecurity Architecture group (discussed below) to create policies and standards that meet compliance requirements and reduce the impact of cybersecurity attacks. The Governance team also oversees the Disaster Recovery and Business Continuity Planning functions, supporting SCE's Business Impact Analysis (BIA) process in collaboration with the Business Resiliency department (discussed in greater detail in SCE-04, Vol. 01).

**2) Cybersecurity Architecture Technology and Operations**

This group is responsible for the core cybersecurity operations of the organization. There are five functional areas that make up this team. The primary goal of the Cyber Threat Intelligence Team (CTI) area is to collect, enrich, and disseminate cyber threat intelligence to help internal and external partners make better informed security decisions. This intelligence is collected from various sources, including via our partnership with the Electricity Information Sharing and Analysis Center, various Government Agencies, Industry partners, and open-source outlets. Priority Intelligence Requirements (PIR) are gathered from various Business Units. The CTI team develops products that will meet these PIRs, such as executive level threat briefings, vulnerability reports, and threat hunting packages to name a few. CTI analysts also serve as subject matter experts for Industry and Government initiated Cyber Intelligence Programs. This group works with internal groups such as support to SCE's Insider Risk Program[37] and conducts red team and penetration testing.[38]

The Cybersecurity Operations Center (CSOC) are boots on the ground. Due to the critical nature of SCE business operations, SCE is faced with daily threats from cyber adversaries looking to cause harm to both SCE and the citizens that rely on SCE services. The SCE CSOC plays an active role to help combat this threat. SCE's CSOC is charged with ensuring the safe and reliable operation of the SCE electric grid and the defense of company Information Technology (IT) and Operational Technology (OT) assets by preventing, detecting, analyzing, and responding to cybersecurity events and incidents. This team manages cyber incidents, which is a critical aspect in maintaining business longevity. Adversaries can compromise the SCE network via phishing attempts, exploiting vulnerabilities in SCE hardware and software, entering through SCE supply chain, and by various other means. If CSOC tools and detections are bypassed and an incident is declared, the CSOC maintains an organized response approach, working to limit potential damage, recovery time, and costs as much as possible. CSOC analysts not only play a vital role if an incident is declared within the SCE environment, but also take

---

[37] Employees, contractors, and other trusted third parties known as "Insiders" present a unique challenge for cybersecurity professionals. These individuals are authorized to use SCE systems and information to fulfill their employment and contractual obligations. However, misuse (either intentional or accidental) of access and trust is very difficult to detect. Accordingly, SCE has created an Insider Risk Program to evaluate, prevent, monitor, detect, and respond to risks posed by insiders.

[38] "Red team and penetration testing" refer to the testing of systems and assets by teams of professionals who are trained and experienced with ethical hacking techniques and who can test the effectiveness of security controls the same as real-world cyber-attackers. In essence, ethical hackers "attack" digital systems and assets in a safe manner in order to find weaknesses and fix vulnerabilities.

proactive action when there is a breach within SCE supply chain. Once an incident is contained, forensic activities are conducted as needed to uncover granular details that are utilized when determining business impact and next steps in the response process.

The SCE CSOC also utilizes network monitoring tools to determine, in part, what devices and applications are on the network. The associated traffic, data, and user access is examined and enriched to detect any abnormal activity that may require further response or forensic investigation. Then, they will leverage available intelligence to "threat hunt," or determine if there is any evidence of adversarial activity within the SCE environment. Relevant detections and tool refinement and enrichment will be put in place to reduce the identified security gaps.

Cybersecurity Architecture looks ahead to ensure strategic alignment with the Cybersecurity BPE's three-to-five-year vision, and align Cybersecurity secure design principals, with SCE's technology landscape for current, emerging, and future requirements to ensure protect, detect, respond and remediation capabilities are established for SCE's critical systems. The Cybersecurity architecture framework structure is intended to align strategic objectives driving continuous improvement in operational safety, reliability, and risk management. It lays the foundation of security and risk management being integrated into enterprise-level architectures in accordance with standards such as NIST SP 800-207 Zero Trust Architecture, The Open Group Architecture Framework (TOGAF) and The Sherwood Applied Business Security Architecture (SABSA).

The last two areas, Cybersecurity Technology and Cybersecurity Tools Engineering ensure that cybersecurity tools and technology are architected with a defense-in-depth methodology, rather than a defined set of tools. Using the most current technology and techniques, the team adjusts to respond to new adversary tactics, techniques and demands as they arise. This area integrates best practices from the NIST Cybersecurity Framework and the MITRE ATT&CK[39] Framework which provides input to creating a robust and well-balanced security infrastructure.

**3) National Security Policy Advocacy and Cybersecurity Awareness Program**

This team serves and shapes SCE's strategic partnerships for industry and government national security policy advocacy, research and development, and coordination. This group works to create productive and proactive partnerships with industry and local, state, and Federal governments to

---

[39] "MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations," https://attack.mitre.org/, *accessed on May 5, 2023*.

leverage the full breadth of capabilities within the sector to address cyber and national security risks. These partnerships are critical to help SCE understand cybersecurity threats, vulnerabilities, and technical mitigation measures as they continue to evolve from a local, state, and federal perspective. They provide valuable input to SCE's other, internally facing cybersecurity programs to help SCE continue to learn and adapt to the evolving cybersecurity landscape while continuing to be efficient and effective in our defenses. SCE's ability to defend against, and mitigate, cybersecurity threats ensures that we are able to provide our customers with reliable service. This group also oversees non-NERC cybersecurity compliance requirements and interfaces with SCE's NERC CIP and IT Operations teams in support of SCE's cybersecurity compliance posture.

Outside of these externally facing functions, SCE's Cybersecurity Awareness Program seeks to create a sustainable security culture by influencing and improving identifiable risky behaviors, in recognition of the fact that informed employees with a strong knowledge of cybersecurity are our first line of defense against cyber-attacks. This function is carried out through an innovative awareness and training program which includes an enterprise-wide phishing program which teaches the workforce of the sophisticated tactics of adversaries and both an enterprise-wide awareness training and a new role-based training for highly targeted roles in the company. Through this program, employees receive periodic emails that mimic the content and characteristics of actual malicious phishing emails, such as links to external websites, malicious attachments, or requests for the employee to provide their SCE login credentials. The tactics and techniques used in the program evolve as adversary tactics also evolve. The emails typically include elements of urgency and or negative consequences if the employee fails to act, as the employees are trained that these are common tactics used by adversaries and attackers. The goal of these "test" phishing emails is for the employee to recognize them as potentially harmful and to report them to SCE cybersecurity. In cases where the employee fails to detect the adversarial tactic and therefore "clicks the link" or "opens the attachment," the employee is notified that the email was a test and further training is provided to the employee regarding the risks and tactics of email phishing. As we learn the pitfalls in employees' responses, we modify our program to target areas where our users are more susceptible to phishing, to increase education in those areas and further mitigate those risks. The program's goal is not only to educate employees to recognize, report and resist attacks, but also to understand the potential impact to themselves, their jobs, and the future of the company.

The functions outlined above also support the following Capital programs:

***Perimeter Defense:*** Perimeter Defense is the first line of defense against cyber-attacks. It is the outer layer of protection for our defense-in-depth approach to cybersecurity. It represents the technologies (e.g., firewalls and intrusion detection systems) and related processes, procedures, hardware, and software to protect critical systems such as SAP, customer data, and ultimately our grid from unauthorized access. When properly configured, the perimeter defenses should only permit those activities required to conduct business. In a perimeter defense security model, the perimeter technology prevents, absorbs, or detects attacks, thereby reducing the risk to critical back-end systems.

In addition, the Perimeter Defense program will continue to refine existing intrusion protection measures and implement new ones (such as systems with deep-scanning capabilities and advanced data analytics capabilities) to better detect unauthorized intrusions. This program will integrate these new tools and controls into our existing Perimeter Defense layer to create common, unified monitoring that lets us rapidly respond to security events including: (1) Identity Governance and Access Management (IGAM); (2) Information Technology/Operational Technology (IT/OT) integration; (3) Foundational Tools; and (4) Labs. More discussions regarding these tools and controls and associated costs are outlined in the forecast analysis sections below.

***Interior Defense:*** Interior Defense comprises protection controls securing SCE's internal business systems from unauthorized users, devices, and software. It also includes the use of analytics to anticipate and prevent attacks from happening. Additionally, Interior Defense helps identify and block security breaches from personnel who have some level of authorized access to the systems.

Users of SCE's business systems can propagate and/or launch malware knowingly or unknowingly. Without the Interior Defense controls, SCE could not identify or react to an infected computer or malicious breach attempting to infect others on the network. By quickly identifying suspicious activity, SCE can take earlier action to minimize any potential damage from the attack.

The Interior Defense mitigation lets us monitor SCE's internal business network, in real-time and with advanced and integrated capabilities. This makes it difficult for unauthorized users to access our systems, and also protects against authorized users knowingly or unknowingly propagating cybersecurity attacks. This mitigation also makes it harder for rogue devices or software to access SCE systems and confidential data or to cause business disruption. This mitigation also addresses advanced threats by using advanced data collection and analysis technologies that can quickly detect potential questionable activity.

To accomplish all of this, the Interior Defense mitigation program:

- Extends SCE's Identity and Access Management system to newer generation security technology;
- Enhances and expands SCE's data collection capabilities to retrieve (and, as needed, collect) disparate pieces of data to form a clear picture of threats and attacks;
- Implements technology capabilities so that SCE can analyze collected information for security threats in a more automated and effective manner; and
- Initiates automated alerts when questionable activity is detected.

***Data Protection:*** The Data Protection program safeguards the computing environment housing SCE's core information. Among other things, this program protects confidential SCE information that resides on all computing devices; this includes protection from unauthorized use, distribution, reproduction, alteration, or destruction.

The Data Protection program leverages specialized technology to better protect and encrypt data fields within files, enhances access controls to protect sensitive business information, and secures business information stored at external sites that host SCE business systems. In addition, this mitigation program implements enhanced controls for granular data protection by deploying Data Loss, Categorization, and Identification tools. These tools will:

- Automate data classification by tying together the different systems that contain data and the ability to classify them;
- Monitor and alert unauthorized access to business information by leveraging the monitoring and data analysis environment with new toolsets;
- Manage business information that is saved on personal devices; and
- Manage and restrict the copying of business information to portable devices.

***SCADA Cybersecurity:*** This program provides enhanced security measures by implementing risk-reduction methods specifically tailored for SCE's SCADA systems. SCE's SCADA systems remotely control and monitor the electric grid.

SCADA Cybersecurity protects legacy and future industrial control systems that are currently connected via routable networks. As threats evolve, SCE must take measures to improve visibility, detection, and protection controls by:

- Building a secure network to protect the administrative interfaces of critical tools;

- Developing device and user access controls to secure user interactions with control systems and to restrict access to the minimum level required for the user's particular role;
- Implementing current generation protections to identify malware;
- Deploying vulnerability management tools to search for and identify known vulnerabilities;
- Providing data encryption services;
- Implementing integration tools to gather intelligence and monitor and analyze potential and actual threats; and
- Procuring government-issued secure technology to defend against advanced attacks.

***NERC CIP Compliance:*** This program is an existing compliance control involving the ongoing implementation of systems and processes to comply with the cybersecurity requirements of NERC CIP. These systems and processes improve how SCE manages facility access, maintains asset change control, and controls physical access. The program focuses on enabling and augmenting the system and processes required for NERC CIP compliance as compared to the other programs above covering standalone security controls. The capital forecast increases include implementation of new NERC CIP controls due to regulatory standards.

**2. Need for Activity**

The energy sector is constantly under threat from well-funded, motivated, and extremely capable foreign adversaries, as well as other threat actors seeking to disrupt the critical supply of energy to Americans. Ensuring the security of Southern California's electric grid has implications that range from the national security risks of disrupting strategic military installations, to the economic risk of disrupting one of the most populated and economically influential regions, down to the individual health, safety, and well-being of individual households, including SCE's customers.

As our adversaries evolve, the attack methods, strategies, and capabilities that they employ are constantly maturing as new types of attacks are discovered and carried out.[40]

---

[40] World Economic Forum, Global Cyber Security Outlook 2022 Insight Report (Jan. 2022) , p. 14. Ransomware attacks saw a significant increase in the first six months of 2021, with global attack volume increasing by 151%. The United States Federal Bureau of Investigation (FBI) has warned that there are now (*Continued*)

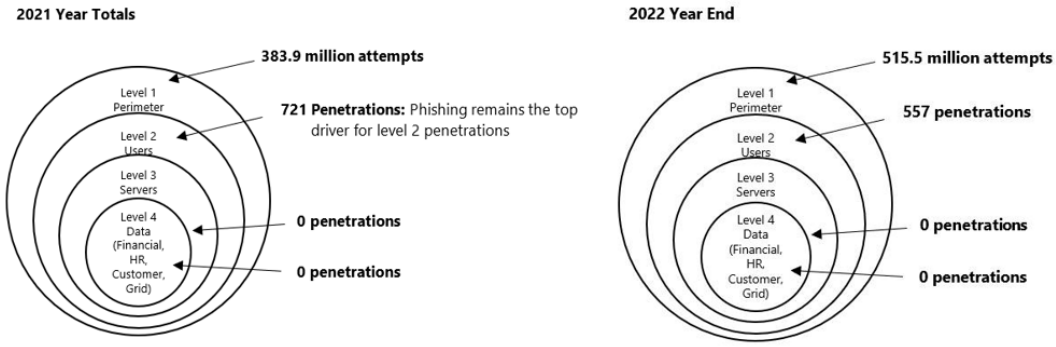
Additionally, SCE's attack surface area, or the number and type of network-attached digital assets and services, continues to grow each year. As noted in the Safety Policy Division Comments section of this document, SCE's number of digital assets and interfaces have increased 50% or more since our prior GRC filing. This growth, combined with increased cyber threat capability and activity, requires considerably more Cybersecurity effort than was necessary just a few years ago. Intrusion attempts against SCE continue to increase, including those which leverage phishing, ransomware, viruses, worms, spyware, and advanced persistent threats. In 2021, for example, as stated in Figure II-6, there were approximately 383.9 million intrusion attempts for SCE's perimeter defense alone. That number grew to almost double (515.5 million attempts) by year end of 2022. However, the number of penetrations via users decreased, meaning that, while the number of *attempts* increased in 2022, the number of attempts that were successful in getting past SCE's defenses (i.e., users falling prey to phishing), decreased. This decrease demonstrates the effectiveness of overall cybersecurity efforts, as described in section II.B.1 Cybersecurity Delivery Project or Program Description above, and the effectiveness of our detection tools. As the number of cybersecurity attacks and assets that must be protected increase exponentially, so must the investments to ensure maturity of our programs and tools. Without these additional investments, it is impossible to adequately protect the security of SCE's customers' data and ensure the delivery of reliable service.

Figure II-6 demonstrates that each of these attacks are no longer theoretical; they pose a real and demonstrated risk to SCE, our systems, and our operations.

---

100 different strains of ransomware in circulation globally. It is unlikely that this issue will diminish in pace or severity any time soon. There were, on average, 270 attacks per organization in 2021. This represents a 31% increase over 2020; *available at* *https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf*

***Figure II-6***
***Intrusion Attempts***




Additionally, a leading cybersecurity vendor released a report on threat groups that have been targeting industrial control systems (ICS) along with specific industries. Of the 15 threat groups detailed in the report, 11 are focused on attacking or gaining access to electric systems. These threat groups target technologies specific to generation, transmission, and distribution operations.[41] This makes electric utilities, like SCE, a prime target for cyberattacks.

In response to the recent attacks and increased threat activity, the U.S. Government has started developing plans and new regulatory requirements that affect utilities and critical infrastructure companies that were previously less regulated in this arena. The U.S. Department of Energy announced a 100-day plan to improve the cybersecurity posture of utilities in April of 2021. This effort aimed to raise awareness of the risk associated with Industrial Control Systems (ICS) and to prioritize the deployment of technology to gain visibility and monitoring within ICS environments.[42] For the organizations related to the pipeline sector, the Transportation Security Agency (TSA) released Security Directive (SD) 02. This provision requires operators of designated critical pipelines to initiate a

[41] Dragos, Global Electric Cyber Threat Perspective (2021)Sep. 2021), *available at* https://hub.dragos.com/hubfs/Reports/Global%20Electric%20Cyber%20Threat%20Perspective%20-%20Dragos%202021.pdf.

[42] Department of Energy, *Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats*, April 20, 2021, *available at* https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0.

cybersecurity program with mandatory reporting and communication requirements.[43] As electric utilities are often dependent on the delivery of fuels from pipeline companies and may have connected or dependent information systems, regulations such as SD02 may be applied or developed for non-CIP regulated companies in the near future. SCE is aware of these programs and the continued attention and scrutiny on cybersecurity across the critical infrastructure landscape and must respond accordingly.

Given the sophistication of cyber threats to our critical infrastructure and the continued focus on cybersecurity throughout the country, SCE must continue and advance cybersecurity work activities to protect our systems. SCE's forecasts reflect the scope of work activities and resources needed to properly position us against cyberattacks. As cyber threats grow, so must our ability to neutralize them. Cybersecurity activities require skilled and knowledgeable personnel. Highly qualified and trained engineers continually study, evaluate and prioritize the utility's resources and infrastructure to keep the grid safe and reliable and to mitigate security risks. SCE actively seeks to recruit and retain such engineers in a limited and competitive labor market. In addition to resources that protect inwardly, resources must be dedicated to collaborating with external partners such as governments and utility peers. Securing the grid requires continuous investment to support SCE's ability to anticipate and mitigate current and future threats with both internal defenses and external partnerships. Additionally, we must continue to invest in strengthening our infrastructure and technology to protect against these threats. SCE's O&M and capital forecasts reflect the scope and level of activities necessary to properly protect SCE's assets and the grid.

### 3. RAMP Integration

#### a) O&M

The work anticipated in the 2025 GRC for Perimeter Defense, Interior Defense, and Data Protection is still the same as the work described in the 2022 RAMP filing. The variance for the 2022 RAMP filing versus the GRC for those controls is due to anticipated delays in spending in 2023 and 2024 as funds are re-allocated to other areas in SCE that were deemed a higher priority. As such, the increases in 2025 are generally offset by decreases in 2023 and 2024. This work is still critical to support an increasing level of cybersecurity preparation while adjusting to new tactics, techniques, and procedures that attackers develop and utilize. This preparation includes upgrading

---

[43] U.S. Dept. of Homeland Security, *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators*, July 20, 2021, *available at* https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

systems, investing in new technologies, training SCE personnel to maintain and enhance their cybersecurity skills, and assessing both current environments and projected future ones. For SCADA Cybersecurity, the variance is explained by additional SCADA cybersecurity consulting and professional services driven by various cybersecurity assessments. Lastly, for Grid Modernization Cybersecurity, the variance is minimal and is explained by normal forecasting refinements. RSE values changed based on moving to the weighted average cost of capital (WACC) for future cost discounting and updated financial forecasts.

***Table II-2***
***RAMP vs. GRC O&M Forecast Comparison***
*(Nominal $000)*[44]
***Risk Spend Efficiencies Comparison***[45]

| RAMP Risk | RAMP ID | RAMP Control / Mitigation Name | Filing | 2022 | 2023 | 2024 | 2025 | 2025 - 2028 RSE |
|---|---|---|---|---|---|---|---|---|
| CyberAttack | C1 | Perimeter Defense | RAMP | $6,617 | $7,677 | $8,441 | $9,723 | 351 |
| | | | GRC | $6,623 | $6,830 | $6,887 | $11,601 | 322 |
| | | | Variance | $5 | ($847) | ($1,554) | $1,878 | (29) |
| CyberAttack | C2 | Interior Protection | RAMP | $3,481 | $4,076 | $4,454 | $5,309 | 477 |
| | | | GRC | $3,090 | $3,494 | $3,560 | $6,463 | 423 |
| | | | Variance | ($391) | ($582) | ($894) | $1,154 | (54) |
| CyberAttack | C3 | Data Protection | RAMP | $3,491 | $4,087 | $4,522 | $5,245 | 460 |
| | | | GRC | $3,213 | $3,729 | $3,759 | $6,502 | 412 |
| | | | Variance | ($278) | ($357) | ($763) | $1,258 | (48) |
| CyberAttack | C4 | SCADA Cybersecurity | RAMP | $1,296 | $1,593 | $1,751 | $2,003 | 796 |
| | | | GRC | $1,173 | $1,362 | $1,418 | $2,383 | 706 |
| | | | Variance | ($123) | ($231) | ($333) | $380 | (90) |
| CyberAttack | C5 | Grid Modernization Cybersecurity | RAMP | $3,659 | $4,509 | $5,082 | $5,804 | 100 |
| | | | GRC | $3,240 | $3,826 | $3,933 | $6,801 | 48 |
| | | | Variance | ($419) | ($683) | ($1,149) | $997 | (52) |

[44] Refer to WP SCE-04, Vol. 03, pp. 29 – 48, Cyber RAMP Integration.

[45] The RSE values are inconclusive of the total O&M and Capital Expenditures for the controls across all applicable GRC activities. SCE cannot readily parse out the RSE by O&M versus. Capital and by the individual GRC activity.

### b) Capital

When comparing SCE's RAMP and GRC Capital estimates, there is a slight increase in the GRC values across all years and all mitigations. These increases are due to slightly higher software and hardware forecasted costs than those included in SCE's RAMP. RSE values changed based on moving to the weighted average cost of capital (WACC) for future cost discounting and updated financial forecasts.

***Table II-3***
***RAMP vs. GRC Capital Forecast Comparison***
*(Nominal $000)*[46]
***Risk Spend Efficiencies Comparison***[47]

| RAMP Risk | RAMP ID | RAMP Control / Mitigation Name | Filing | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 | 2025 - 2028 Total Spend | 2025 - 2028 RSE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CyberAttack | C1 | Perimeter Defense | RAMP | $38,900 | $36,900 | $40,010 | $41,259 | $42,387 | $43,537 | $44,718 | $171,902 | 351 |
| | | | GRC | $46,395 | $36,917 | $40,679 | $41,965 | $43,097 | $44,160 | $45,249 | $174,470 | 322 |
| | | | *Variance* | $7,495 | $18 | $669 | $706 | $710 | $622 | $531 | $2,569 | (29) |
| CyberAttack | C2 | Interior Protection | RAMP | $8,100 | $8,100 | $8,100 | $8,100 | $8,321 | $8,547 | $8,779 | $33,748 | 477 |
| | | | GRC | $5,172 | $8,102 | $8,232 | $8,230 | $8,451 | $8,660 | $8,874 | $34,215 | 423 |
| | | | *Variance* | ($2,928) | $2 | $132 | $130 | $130 | $113 | $95 | $468 | (54) |
| CyberAttack | C3 | Data Protection | RAMP | $8,600 | $12,400 | $12,400 | $12,400 | $12,739 | $13,085 | $13,440 | $51,663 | 460 |
| | | | GRC | $10,767 | $12,406 | $12,608 | $12,613 | $12,954 | $13,273 | $13,601 | $52,441 | 412 |
| | | | *Variance* | $2,167 | $6 | $208 | $213 | $215 | $188 | $161 | $778 | (48) |
| CyberAttack | C4 | SCADA Cybersecurity | RAMP | $2,498 | $2,498 | $2,498 | $2,498 | $2,566 | $2,636 | $2,707 | $10,408 | 796 |
| | | | GRC | $2,342 | $2,499 | $2,540 | $2,542 | $2,610 | $2,675 | $2,741 | $10,567 | 706 |
| | | | *Variance* | ($156) | $1 | $42 | $44 | $44 | $39 | $33 | $160 | (90) |

## 4. Comparison of Authorized 2021 to Recorded

### a) O&M

SCE was authorized $23.6 million in O&M expenditures for Cybersecurity & Compliance activities in the 2021 GRC test year. The recorded 2021 O&M expenses for these activities was $18.8 million, which was $4.8 million below the authorized amount.

In 2021, SCE continued to experience the global impact of the COVID-19 pandemic. Therefore, SCE made necessary adjustments to normal operations and practices in an effort to

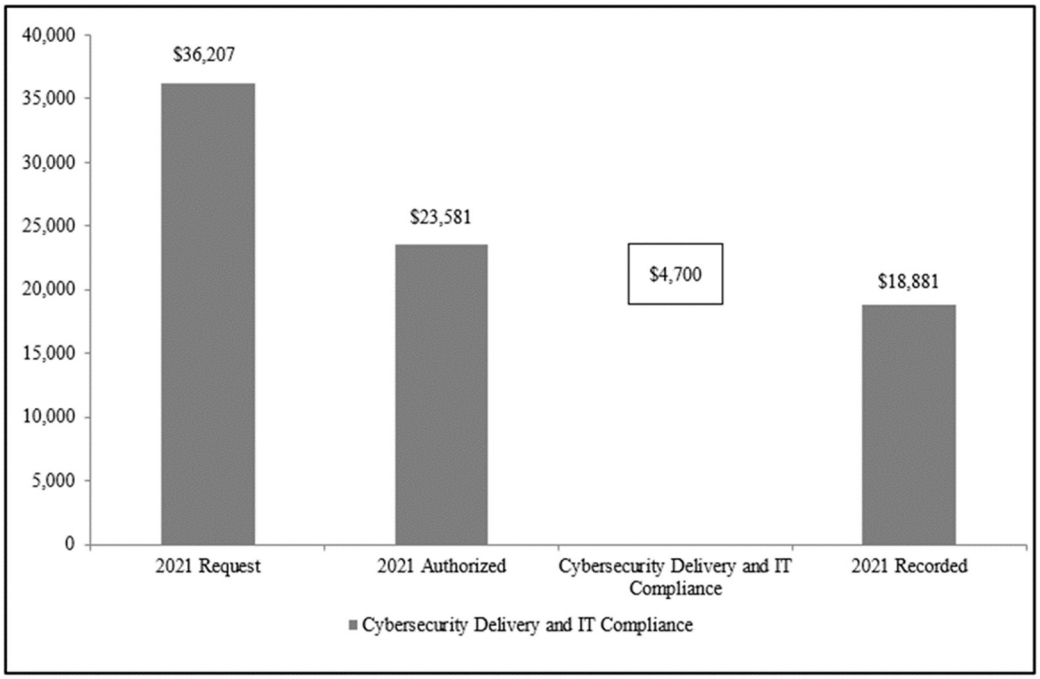
---

46 Refer to WP SCE-04, Vol. 03, pp. 29 – 48, Cyber RAMP Integration.

47 The RSE values are inconclusive of the total O&M and Capital Expenditures for the controls across all applicable GRC activities. SCE cannot readily parse out the RSE by O&M vs. Capital and by the GRC activities and by the individual GRC activity.

mitigate the risk of COVID-19 transmittal and spread, and in order to comply with COVID-driven governmental directives and guidance. Some of these adjustments by SCE impacted to a degree our ability to rapidly fill open positions, as well as the scope of activities related to business travel, attending job-related or industry-related conferences, or engaging in normal levels of in-person training. As a result of the protocols that we necessarily adopted during the pandemic, the recorded expenses for this activity in 2021 were lower than authorized.

***Figure II-7***
***Cybersecurity Delivery***[48]
***Comparison of 2021 Authorized versus Recorded O&M Expenses***
*(Constant 2022 $000)*




**b) Capital**

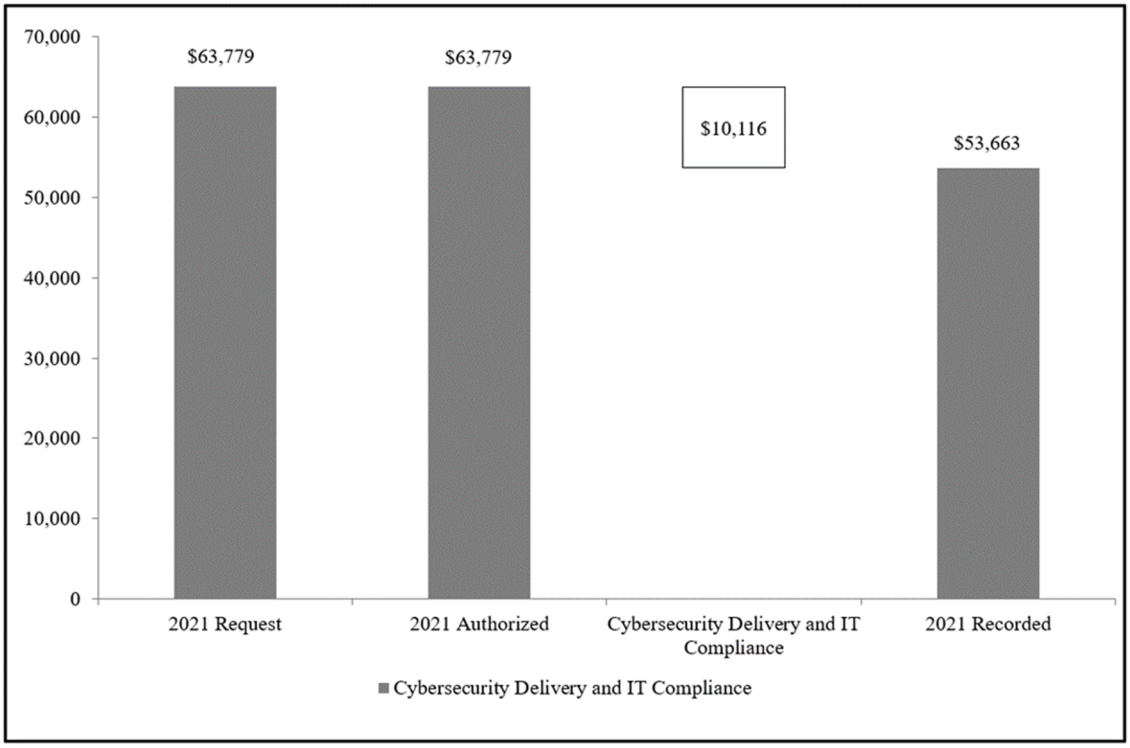
In the 2021 GRC test year, the Commission authorized $63.779 million for Cybersecurity Delivery. SCE recorded Cybersecurity Delivery expenditures of $53.663 million in the 2021 test year, which is $10.116 million less than authorized. The variance arose from delays in our

[48] *See* WP SCE-07, Vol. 01, Authorized vs. Recorded.

Data Protection and Perimeter Defense programs as funds for these programs, as described above, are re-allocated to other areas in SCE that were deemed a higher priority.

In addition, and as with its O&M costs, SCE's capital costs continued to be impacted by the global impact of the COVID-19 pandemic in 2021. Therefore, SCE made necessary adjustments to normal operations and practices in an effort to mitigate the risk of COVID-19 transmittal and spread, and in order to comply with COVID-driven governmental directives and guidance. Some of these adjustments by SCE impacted to a degree our ability to execute projects. As a result of the protocols that we necessarily adopted during the pandemic, the recorded expenses for this activity in 2021 were lower than authorized.

***Figure II-8***
***Cybersecurity Delivery***[49]
***Comparison of 2021 Authorized versus Recorded Capital Expenditures***
*(Nominal $000)*




[49] *See* WP SCE-07, Vol. 01, Authorized vs. Recorded.

## 5. Scope & Forecast Analysis

### a) Historical Variance Analysis

#### (1) Labor

***Table II-4***
***Cybersecurity Delivery O&M Expenses***[50]
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $9,752 | $10,160 | $13,387 | $13,669 | $13,416 | $14,756 | $14,631 | $21,037 |
| *Non-Labor* | $6,859 | $5,641 | $3,842 | $5,212 | $6,517 | $4,151 | $3,986 | $10,090 |
| *Other* | | | | | | | | |
| Total Expenses | **$16,611** | **$15,801** | **$17,229** | **$18,881** | **$19,933** | **$18,907** | **$18,616** | **$31,127** |

SCE's cyber workforce strategy of recruiting new talent and retaining skilled staff members with specialized cybersecurity expertise is necessary to support our efforts to address new and emerging cyber threats. According to the US Bureau of Labor Statistics,[51] between 2018 and 2021 (the latest year for which data is presently available), the number of Information Security Analysts in the Los Angeles area increased by 33%. In that same period, average salaries for Information Security Analysts in the Los Angeles area increased 17%, as compared to 11% for the nation overall. Also notable is that the national average salary for Information Security Analysts working for Utilities increased 27% between 2018 – 2021. Reflective of that state, labor costs for Cybersecurity Delivery steadily increased from 2018 to 2022, as key staff additions to the Cybersecurity & IT Compliance teams were necessary for reinforcement of cybersecurity controls and data protection capabilities.

Despite increases in wages, an ongoing challenge to SCE's cyber workforce strategy, and one discussed in prior GRC submissions,[52] is attracting, and retaining cybersecurity professionals. In 2021, a Cybercrime Magazine report[53] predicted there would be 3.5

---

[50] Refer to WP SCE-04, Vol. 03, pp. 16 – 28, Cybersecurity Delivery – Standard Workpapers.

[51] Refer to WP SCE-04, Vol. 03, pp. 49 – 50, Bureau of Labor Statistics, Occupational Employment and Wage Statistics, *available at* https://www.bls.gov/oes/tables.htm.

[52] *See* SCE-04, Vol. 03, Cybersecurity & Compliance Testimony in 2021 GRC.

[53] Steve Morgan, *Cybersecurity Jobs Report: 3.5 Million Openings In 2025,* CYBERCRIME MAGAZINE, April 14, 2023, *available at* https://cybersecurityventures.com/jobs.

million unfilled cybersecurity jobs globally in 2025, which is a 350% increase from 2014. This same article reported that in the U.S. there are just over 90,000 individuals with CISSP (Certified Information Systems Security Manager) certification, but more than 106,000 job openings requiring a CISSP certification. Furthermore, the article also noted there are 17,000 CISMs (Certified Information Security Managers) in the U.S., but nearly 40,000 advertised jobs requesting the CISM certification. SCE's experience in the 2018 to 2021 period matches what was reported in these articles. Individuals with the requisite cybersecurity expertise, with these preferred certifications, were in short supply. Identifying and hiring qualified candidates was prolonged, requiring SCE to prioritize and shift cyber staff assignments and to supplement its cybersecurity work with non-labor resources to ensure access to the hard-to-find expertise required to address the most urgent needs and critical risks.

**(2) Non-Labor**

***Table II-5***
***Cybersecurity Delivery O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $9,752 | $10,160 | $13,387 | $13,669 | $13,416 | $14,756 | $14,631 | $21,037 |
| *Non-Labor* | $6,859 | $5,641 | $3,842 | $5,212 | $6,517 | $4,151 | $3,986 | $10,090 |
| *Other* | | | | | | | | |
| Total Expenses | **$16,611** | **$15,801** | **$17,229** | **$18,881** | **$19,933** | **$18,907** | **$18,616** | **$31,127** |

The non-labor costs in 2018 reflected a spike of $3.3 million due to an accounting change causing hardware maintenance costs to be moved from Capital to O&M consistent with SCE accounting practices.[54] In 2018, non-labor costs increased as the previously delayed initiatives moved forward. Non-labor cost increases in 2018 were also driven by compliance activities associated with the increasing volume of state and federal cybersecurity and compliance requirements and a significant growth in volume and complexity of cybersecurity intrusion attempts. This resulted in greater utilization of outside resources to support cybersecurity assessments and to supplement hard to find FTE resources due to talent shortages which is expected to continue going forward. According to the International Information System Security Certification Consortium ((ISC)$^2$) 2022 Cybersecurity

[54] Please refer to 2021 GRC SCE 07, Vol. 01 for SCE's accounting practices.

Workforce Study,[55] it is estimated that in the United States there is a deficit of 410,695 cybersecurity positions, which has grown 9% year-over-year from 2021. The year 2019 did not reflect the one accounting rule change, thus there was a slight decrease of $1.218 million, offset by increasing needs to continue to drive compliance activities associated with federal cybersecurity and compliance requirements with the support of supplemented contract workers.

As discussed above in Labor, an ongoing challenge to SCE's cyber workforce strategy is shortage of individuals with the requisite cybersecurity expertise in IT/OT integration. In 2020, we also faced this challenge in our contractor workforce, therefore contributing to a decrease of $1.799 million from the prior year.

In 2021, the spend reflected an increase of $1.370 million as Cybersecurity & Compliance once again supplemented staff to support risk mitigation efforts in cyber operations. In 2022, the spend increased further by $1.305 million due to the need, once again, for supplemented contract workers to support risk mitigation efforts and operational projects in cybersecurity.

**(3) Capital**

***Table II-6***
***Cybersecurity Delivery Capital Expenditures***[56]
***2018-2022 Recorded / 2023-2028 Forecast***
*(Nominal $000)*

| | Recorded | | | | | Forecast | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 |
| Cybersecurity Delivery and IT Compli | $33,485 | $44,701 | $39,453 | $53,663 | $66,833 | $64,429 | $66,605 | $67,905 | $69,737 | $71,457 | $73,220 |
| Totals | $33,485 | $44,701 | $39,453 | $53,663 | $66,833 | $64,429 | $66,605 | $67,905 | $69,737 | $71,457 | $73,220 |

Consistent with SCE's prior GRCs, the volume and complexity of Cybersecurity Delivery and IT Compliance capital expenditures varying from year to year is driven by system refresh and obsolescence and additional new functionalities needed to address increasing threats, which drove the fluctuations between 2018-2022.

Capital costs increased from $33.485 million to $44.701 between 2018 to 2019. This is mostly attributable to the increase in investments of Perimeter Security Technologies and

---

55 (ISC)$^2$, Cybersecurity Workforce Study, A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution, p. 8 (2022), *available at* https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.

56 Refer to WP SCE-04, Vol. 03, pp. 16 – 28, Cybersecurity Delivery – Standard Workpapers.

related implementation services to support emerging threats and organic growth within Information Technology.

In 2020, capital spend decreased to $39.453 million due to fewer legacy systems being refreshed that year. Capital expenditures increased to $53.663 million in 2021 due to investments in remote tools to accommodate security advancement to support remote work. Also, more legacy technologies required a refresh in 2021.

Finally, the Capital increase of $13.2 million in 2021 to $66.833 million in 2022 is attributed to third party price increases of 15% across hardware, software, and contract labor. Moreover, additional cost drivers included an increased emphasis on attack surface monitoring and legacy technologies requiring refresh.

**b) Basis of Forecast**

**(1) Labor**

***Table II-7***
***Cybersecurity Delivery O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $9,752 | $10,160 | $13,387 | $13,669 | $13,416 | $14,756 | $14,631 | $21,037 |
| *Non-Labor* | $6,859 | $5,641 | $3,842 | $5,212 | $6,517 | $4,151 | $3,986 | $10,090 |
| *Other* | | | | | | | | |
| Total Expenses | **$16,611** | **$15,801** | **$17,229** | **$18,881** | **$19,933** | **$18,907** | **$18,616** | **$31,127** |

SCE utilized the 2022 recorded labor costs of $13.416 million as the initial basis of our test year forecast. Consistent with our RAMP Report, SCE anticipates an increase of $7.621 million in 2025 to its 2022 costs for O&M labor to manage additional and/or new risks in several key areas for a total 2025 Test Year forecast of $21.037 million.

The risk of cyberattacks has changed significantly due to global politics and the associated actions of nation-states. Cyberattacks are evolving at a rapid pace, and the mitigations that worked against previous attacks may not be as effective against future attempts. Cybersecurity threats can originate from virtually anywhere across the world. Cybersecurity challenges can also be triggered or motivated by social unrest, political differences and upheavals, and religious and cultural factors.

Several efforts driving the labor forecast attempt to address what we know about our existing defenses, the demographics and capabilities of our attackers, and the growth and complexity of the attacks we will face in the future. Examples of areas where SCE will be bolstering its efforts in the coming years include expanded cybersecurity engineering, architecture, system design, governance, and risk functions. A non-exhaustive list of examples is discussed below.

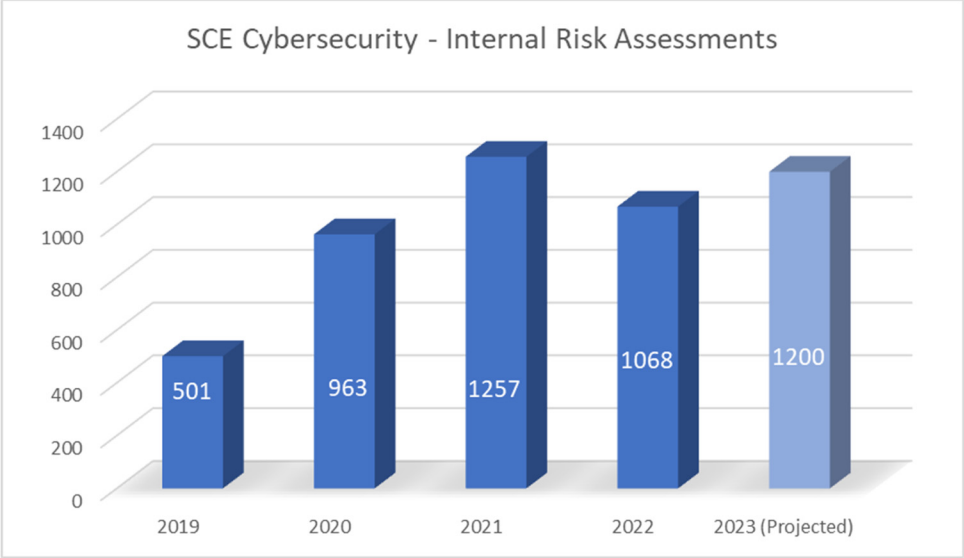
A significant area of risk is the increased Information Technology (IT) to Operational Technology (OT) integration as SCE's cybersecurity perimeter grows beyond our datacenters and into substations and field devices. This IT/OT convergence significantly increases SCE's cyber-attack surface, so cybersecurity engineering, architecture, and design activities are increasing in both quantity and complexity. For example, SCE has been piloting Early Fault Detection (EFD) sensors[57] on utility poles. These sensors "listen" to power signals crossing the electrical lines with the intent of identifying potentially hazardous line conditions that could lead to wildfires, etc. In order to report anomalies, these sensors must be connected to SCE's network. Given the potential for thousands of these devices, and the fact that they can be physically accessed by anyone with a ladder and crowbar, cybersecurity protections must ensure that they cannot be used as a conduit into SCE's OT or IT networks. This is accomplished through thorough cybersecurity architecture design, risk assessments and penetration testing, continuous cybersecurity monitoring of the sensors, and ongoing vulnerability management and patching of the sensors as vulnerabilities are discovered and reported by the vendor. This is just one example of how SCE's network is expanding beyond traditional datacenters and substations. Datacenters and substations afford SCE a better ability to restrict physical access to network-attached assets, whereas utility pole-mounted assets are numerous, easily accessible, and challenging to monitor for unauthorized physical access. As is necessary for proper and consistent operations, Cyber Governance and Risk headcount must also increase to match the larger scale of support needed for these new initiatives.

---

[57] Refer to WP SCE-04, Vol. 03, pp. 51 – 56, David Song, *New Technology Sounds the Alarm on Wildfire Hazards*, ENERGIZED, February 5, 2021, *available at* https://energized.edison.com/stories/new-technology-sounds-the-alarm-on-wildfire-hazards.

As demonstrated in Figure II-7, SCE's Cybersecurity organization has experienced a 240% increase in internal demand for cyber risk assessments[58] since 2019, as a result of the digitization of the Grid. COVID-driven initiatives to enable employees to effectively work from home also drove a sharp increase in the number of cybersecurity assessments in 2021. Despite the higher than usual volume in 2021, the growing need for these assessments is quite evident, as is the need for additional SCE labor and contractor support for these activities.

***Figure II-9***
***Internal Cybersecurity Risk Assessments***




Enhanced monitoring capabilities are needed for increased grid and administrative network monitoring. Increased numbers of networks and devices will bring a higher number of alerts, analysis, investigations, and tuning. The increased scope and scale will require additional headcount beyond current staffing levels.

In addition, the modernizing the grid will require a Zero Trust[59] security architecture, due in part to the increased IT/OT convergence. As such, cyber architecture and design activities will include additional network segmentation, identity and access management, network and

[58] "Internal risk assessments" refers to standards-based evaluations of cybersecurity risks and cybersecurity controls for new, existing, and upgraded hardware, software, systems, platforms, etc. These assessments may also include vulnerability and/or penetration testing activities.

[59] Microsoft states that Zero Trust incorporates three principles: 1) verify explicitly, 2) use least-privileged access, and 3) assume breach. *Available at* https://www.microsoft.com/en-us/security/business/zero-trust.

endpoint protection, and data security. Data security includes discovery, data classification, and classification-specific data protection. Zero-Trust Architectures were the focus of a 2022 White House Memorandum addressing the need to modernize the Federal Government's approach to security. The memo includes a reference to the Department of Defense Zero Trust Reference Architecture which states "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction."[60]

Additional vulnerability management and testing is also necessary due to the extensive increase in the number and variety of assets needed to power a carbon-neutral electrical grid. With increased number and variety of assets necessary to enable a modernized grid, vulnerability management and testing also become more difficult. The Cybersecurity and Infrastructure Security Agency (CISA) publishes over 11,000 Common Vulnerabilities and Exposures (CVEs)[61] each year, including over 1,700 CVEs for OT and Industrial Control Systems.[62] Once released, owners of vulnerable hardware and software must gauge the potential impact(s) of the device to SCE's network, assign priority, and act to patch systems and assets before they become discovered by attackers. A greater variety of assets means additional effort to discover, review, and patch vulnerable systems, as well as perform vulnerability scans and testing to ensure systems are properly patched, requiring increased headcount.

Finally, to address Supply Chain Risk Management issues requires additional personnel to proactively monitor and manage an estimated 2200 vendors' cybersecurity posture based on the vendor's criticality to SCE's operations. As noted previously in this testimony, between the 2021 GRC and this 2025 GRC, SCE's number of on-premise licenses, SaaS and Cloud

---

60 Shalanda D. Young, EXECUTIVE OFFICE OF THE PRESIDENT, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022, *available at* https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

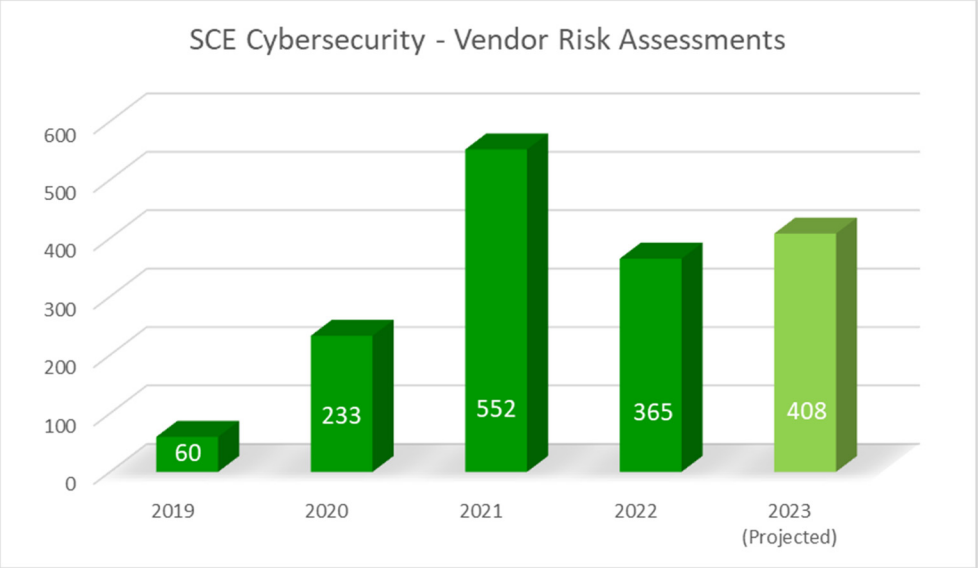
61 Palo Alto Networks, 2022 Unit 42 Network Threat Trends Research Report (Vol. 1, 2022), *available at* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/unit42-network-threat-research-report-vol1.pdf.

62 Dragos 2021 ICS Cybersecurity Year in Review, p. 58 (2021), *available at* https://www.dragos.com/year-in-review/.

subscriptions has grown by 52%.[63] This growth is indicative of a broader increase in use of third-party vendors. Accordingly, SCE's existing resources are insufficient to address the increasing workload associated with a greater number of supply chain vendors.

Similar to the increase in internal risk assessments noted above (Figure II-7), SCE's cybersecurity team has also experienced a 680% increase in vendor risk assessments,[64] as depicted in Figure II-8. These vendor risk assessments are critical for reducing and managing risk across an expanding portfolio of vendors and vendor services. The data represented in Figure II-8 reflects a COVID-driven increase in vendor risk assessments in 2021. Beyond the steep increase in 2021, the growth trend across this 2019 – 2023 period is strongly evident.

***Figure II-10***
***Vendor Risk Assessments***



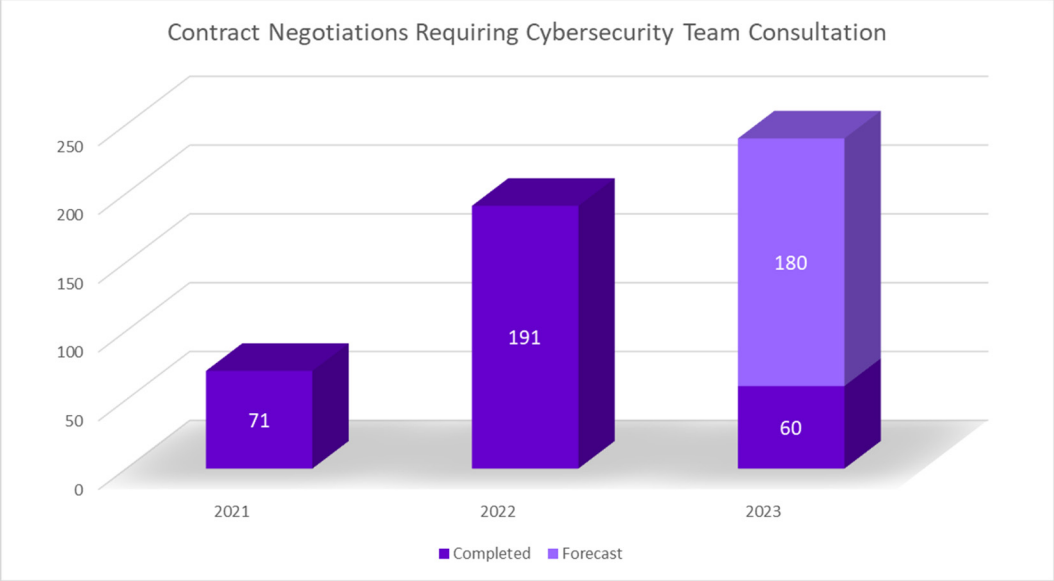

In addition to the vendor risk assessments depicted in Figure II-8, SCE's cybersecurity team is part of SCE's larger team negotiating cyber risk reduction for new and renegotiated contracts based on the third party's risk profile. For example, if SCE were contracting with

[63] SCE IT managed 460 license/subscriptions contractual agreements in the 2021 GRC, while in the 2025 GRC this number increased to 700 contractual agreements. This growth is detailed in SCE-06, Vol. 01, Enterprise Technology.

[64] "Vendor risk assessments" refers to evaluations of vendor cybersecurity practices and capabilities based on the types of service the vendor provides, as well as the types of data and system access, they require to fulfill their contractual obligations.

an accounting firm to support tax filings, the cybersecurity team would evaluate the types of data the external firm will be provided, or have access to, and will also review the contract terms for obligations such as cybersecurity data protection, cybersecurity breach notification, data retention limitations, etc. As contractual terms are negotiated, the cybersecurity team often proposes alternate or modified terms to balance risk exposure and feasibility. Figure II-9 reflects the cybersecurity team's growing involvement in contract negotiations. Furthermore, SCE forecasts another 67% growth in contract negotiations between 2022 and 2025. These increases reflect SCE's need for additional resources to meet this increasing demand for knowledgeable and experienced cybersecurity professionals.

***Figure II-11***
***Contract Negotiations***




While these are just a few examples of the need for additional personnel to address complex cyber risks, we also recognize challenges in hiring cybersecurity talents. SCE is partnering with additional external sourcing agencies specializing in recruiting for cyber technical positions to supplement a dedicated internal team of recruiters in our human resources department to identify and source talent. Additionally, we are increasing our marketing and networking efforts in order

to source these talents in a timely manner. For additional details regarding our labor forecast, please see supplemental work papers.[65] [66]

**(2) Non-Labor**

***Table II-8***
***Cybersecurity Delivery O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $9,752 | $10,160 | $13,387 | $13,669 | $13,416 | $14,756 | $14,631 | $21,037 |
| *Non-Labor* | $6,859 | $5,641 | $3,842 | $5,212 | $6,517 | $4,151 | $3,986 | $10,090 |
| *Other* | | | | | | | | |
| Total Expenses | **$16,611** | **$15,801** | **$17,229** | **$18,881** | **$19,933** | **$18,907** | **$18,616** | **$31,127** |

For Test Year 2025, SCE forecasts non-labor expenses of $10.090 million as shown in Table II-8. Over the last three recorded years, SCE sees a trend of increasing historical spend due to risk mitigation efforts. Consistent with those years and given that we expect the trend to continue, SCE believes that this work activity warrants an itemized forecast to properly reflect the impact of new Cybersecurity initiatives planned in the future.

Similar to prior years, SCE expects to require higher levels of consultant support starting in 2025 for technical expertise and supplementation of cyber skillsets, which is expected to continue through the end of this GRC period. Although SCE does expect an increase in labor to address the needs across the Cybersecurity program, higher levels of consultant support are still necessary because utilizing subject matter experts with existing knowledge of ICS cybersecurity expertise—especially consultants who have worked with other utilities on a variety of similar projects and initiatives—allows them to bring in that experience and multi-organizational insights for SCE's and our customer's benefit. In addition, the experience of consultants minimizes the need for spin up, re-training, and familiarization with the industry, all of which require tremendous time and effort.

---

[65] Refer to WP SCE-04, Vol. 03, pp. 57 – 73, Cybersecurity Delivery 2023-2028 O&M Labor and Non-labor Workpapers. The forecast also incorporates an increase attributable to an adjustment to reflect certain changes made to SCE's employee compensation program. Please refer to SCE-06, Vol. 04.

[66] Note that SCE's Cybersecurity & IT Compliance organization continues to assess efficiencies regarding labor to keep costs down in the midst of facing demands causing our labor growth. This is evidenced by our recent reassessment and consolidation of IT compliance functions that yielded savings of approximately $167,000 per year.

As part of the RAMP Report, SCE detailed several drivers[67] requiring the utilization of outside expertise and skillsets. Some examples of forecasted non-labor costs (previously identified through RAMP) include:

**Standard Cybersecurity Control Baselines** – engagement with a professional services vendor for the creation and implementation of repeatable cybersecurity standards that can be used for all project plans. These standards will provide the project team with common cybersecurity controls appropriate for their specific type of project. The benefit of these standards is that cybersecurity risks and mitigations will be considered from the earliest stages of the project lifecycle. While these consultants will not replace the role of a cybersecurity advisor to the project, they have a national view of what others in the industry are doing in this space which will help advisors be more effective and efficient in not reinventing the wheel. In addition, these efforts happen only periodically and at a one-time basis, so it is more cost efficient to hire consultants, than to hire an additional SCE employee.

**Non-Complex Contract Terms Negotiation** – SCE's Cybersecurity Delivery team supports vendor contract reviews and terms negotiations based on the vendor's risk profile. As noted in Figure II-9, the number of contract negotiations supported by SCE's Cybersecurity Delivery team has grown 338% over the last three years. SCE's approach to address this increase involves adding labor to support complex contract negotiations, while simultaneously outsourcing non-complex[68] contract negotiations to optimize overall spending. SCE intends to outsource the non-complex contract negotiation process to a professional services company that can implement a repeatable process and leverage dedicated resources operating under a Service Level Agreement (SLA). This approach will be more cost effective and more agile than having the SCE cyber team perform these duties in addition to their other responsibilities. If a contract support budget for this activity is not approved, additional labor resources will be needed to cover the additional workload.

---

[67] The primary drivers for RAMP cybersecurity are: 1) External Actors, 2) Insider Threats, and 3) Supply Chain.

[68] "Non-complex" contract negotiations involve application of standard concepts, principles, and terms to contracts for low to medium risk services. "Complex" contract negotiation services involve the potential for significant risk, or for contractual agreements where standard terms cannot be applied or are insufficient for the contacting parties. An example of a non-complex contract might include janitorial services where the contracted staff have limited access or exposure to confidential information, or where SCE could insist that the vendor agree to our standard terms as a condition of contracting.

Beyond the RAMP driven initiatives, SCE requires support from external security consultants. External security consultants offer unique value in this regard, as they bring concentrated expertise in key areas such as IT/OT integration, network segmentation, vulnerability management, and secure architectures. This concentrated expertise comes from performing similar projects for other organizations at a rate of occurrence not possible for SCE employees. These consultants bring lessons learned through multiple industry projects, thus reducing project execution risk for SCE. Furthermore, utilization of consultants that have worked on other large-scale initiatives allows SCE to have access to a large pool of experts with diverse skills, to fit the needs of the specific project. Additionally, focused specialization consultants will continue to be utilized for large and complex initiatives, and as resources for independent assessments of our technical controls serving as both a proactive defense strategy in conformity with industry best practices and a way to leverage outside experience supporting the broader industry.

The justification for this non-labor O&M increase is similar in magnitude to the labor O&M for the same reasons as labor O&M: SCE has a tremendous about of work to do to transform our infrastructures to enable renewable energy as mandated by the State of California by 2045.[69] This initiative will require more monitoring and detection capabilities, more risk and vulnerability assessments, and more processes to enable clean, renewable, and distributed energy generation integrated into our grid, and we must engage external consultants to achieve these goals.

Also, as noted earlier, the growth in volume and complexity of cyber intrusion attempts, and the need to comply with a growing breadth of state and federal cybersecurity and compliance requirements, is expected to continue through 2025 and beyond. Consistent with the RAMP Report, SCE forecasts a higher and recurring need to utilize outside consultants to perform additional evaluations of our Cybersecurity programs.

For additional details, please see supplemental work papers.[70]

---

[69] California Senate Bill 100, titled "The 100 Percent Clean Energy Act of 2018" sets a 2045 goal of powering all retail electricity sold in California with renewable and zero-carbon resources such as solar and wind. Further, it updates the state's Renewables Portfolio Standard to ensure that by 2030 at least 60 percent of California's electricity is renewable. This legislation requires the Energy Commission, Public Utilities Commission, and Air Resources Board to use programs under existing laws to achieve 100 percent clean electricity and to issue a joint policy report every four years starting in 2021. *See* https://www.energy.ca.gov/sb100.

[70] Refer to WP SCE-04, Vol. 03, pp. 57 – 73, Cybersecurity Delivery 2023-2028 O&M Labor and Non-labor Workpapers.

### (3) Capital

***Table II-9***
***Cybersecurity Delivery Capital Expenditures***
***2018-2022 Recorded / 2023-2028 Forecast***
*(Nominal $000)*

| | Recorded | | | | | Forecast | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 |
| Cybersecurity Delivery and IT Compli | $33,485 | $44,701 | $39,453 | $53,663 | $66,833 | $64,429 | $66,605 | $67,905 | $69,737 | $71,457 | $73,220 |
| **Totals** | **$33,485** | **$44,701** | **$39,453** | **$53,663** | **$66,833** | **$64,429** | **$66,605** | **$67,905** | **$69,737** | **$71,457** | **$73,220** |

The total forecasted Cybersecurity Delivery capital expenditures for 2023 to 2028 is $413.353 million. The year-over-year increase between 2023 and 2028 is between 2% and 3%. This is due to the increases in vendor pricing for hardware, software, and services, driving capital costs higher than inflation alone. The forecast reflects the continuing investments necessary for SCE's NERC CIP, Perimeter Defense, Data Protection, Interior Defense, and SCADA Cybersecurity programs.[71]

For each project within the Cybersecurity Delivery activity, the cost is determined by scope and complexity of each activity and historical costs of like activities within NERC CIP, Perimeter Defense, Data Protection, Interior Defense, and SCADA Cybersecurity programs. These projects are then categorized and prioritized based on the activities' risk, urgency, and magnitude of impact. The increases in dollars over the historical period is driven by the following factors:

- Perimeter Defense – as SCE's perimeter expands beyond its traditional boundaries to support greater numbers and types of assets, including IT, OT, and third-party integration, additional capital investments are required.
- IGAM – continued migration of systems to incorporate newer Identity and Access Management as well as Privileged Access Management.
- Increased and more complex threats as described throughout this volume.

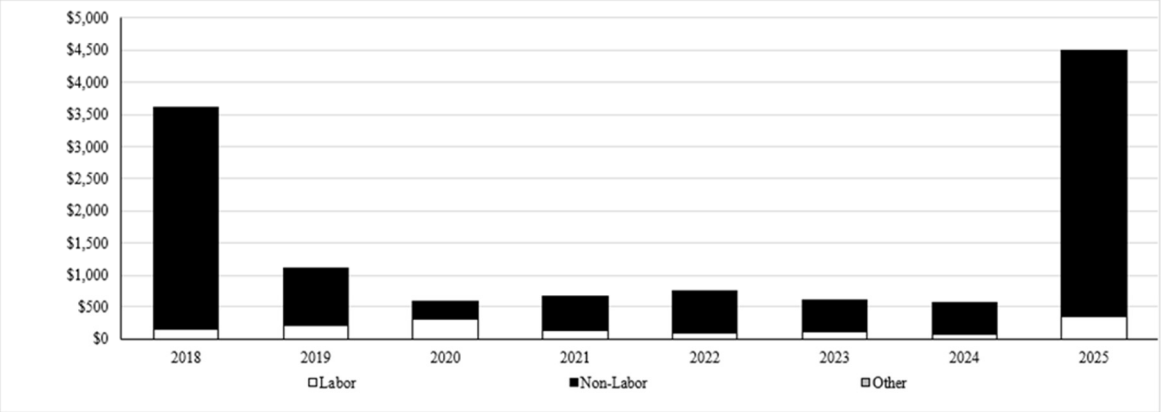
---

[71] Refer to WP SCE-04, Vol. 03, pp. 74 – 80, Cybersecurity Delivery 2023-2028 Capital Programs Workpapers.

## C. Grid Modernization Cybersecurity

Figure II-12 shows 2018-2022 recorded costs and the Test Year 2025 forecast for the Grid Modernization Cybersecurity activity.

***Figure II-12***
***Grid Modernization Cybersecurity O&M Expenses***[72]
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

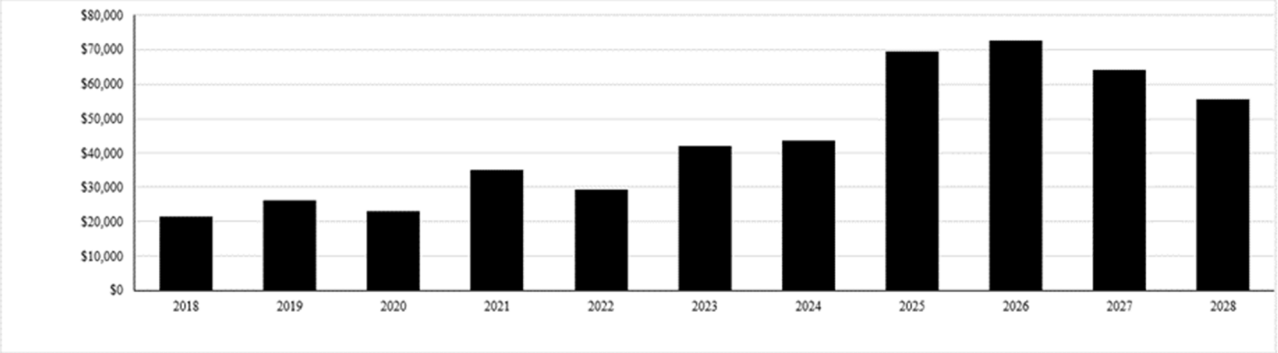



| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $156 | $216 | $318 | $127 | $105 | $115 | $75 | $352 |
| *Non-Labor* | $3,446 | $892 | $269 | $530 | $657 | $481 | $491 | $4,135 |
| *Other* | | | | | | | | |
| Total Expenses | **$3,602** | **$1,108** | **$586** | **$657** | **$762** | **$596** | **$567** | **$4,487** |

Figure II-13 shows 2018-2022 recorded expenditures and the 2023-2028 capital forecast for the Grid Modernization Cybersecurity activity.

72 Refer to WP SCE-04, Vol. 03, pp. 81 – 88, Grid Modernization Cybersecurity – Standard Workpapers.

***Figure II-13***
***Grid Modernization Cybersecurity***[73]
***Capital Recorded /Forecast***
*(Nominal $000)*




| | Recorded | | | | | Forecast | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 |
| Grid Mod Cybersecurity | $21,267 | $26,136 | $22,892 | $35,256 | $29,018 | $41,971 | $43,694 | $69,227 | $72,385 | $63,969 | $55,527 |
| **Totals** | **$21,267** | **$26,136** | **$22,892** | **$35,256** | **$29,018** | **$41,971** | **$43,694** | **$69,227** | **$72,385** | **$63,969** | **$55,527** |

## 1. Project or Program Description

The Grid Modernization Cybersecurity program[74] focuses on addressing the comprehensive security and data protection needs of all new infrastructure and application assets being added through SCE's Grid Modernization program. This activity is necessary to prepare SCE's systems and operational processes to achieve California's 2045 mandate and is focused on improving bulk power management, integration of Grid and customer devices, integrated load management strategies, and customer electrification adoption and affordability.

Despite the implementation of strong preventative controls, cybersecurity for grid modernization designs must account for the possibility that compromises of SCE's network will inevitably occur. A compromised system on the grid enables an avenue of attacks to escalate privilege, launch malware attacks, or render a grid system inoperable. Preventative controls will be imperative in defending SCE's infrastructure and possessing the ability to identify when a compromised system behaves anomalously and execute an automated response to isolate the system and minimize its potential

[73] Refer to WP SCE-04, Vol. 03, pp. 81 – 88, Grid Modernization Cybersecurity – Standard Workpapers.

[74] Given the sensitive nature of cyber security information, only limited content is being presented in this public document. Specific details can be provided to the Commission in confidential briefings as discussed above.

impact to grid operations. This program's scope addresses the multiple layers of technology, vulnerability testing, resources, processes, and procedures that are necessary which include:

- Grid Data Center Cybersecurity foundational capabilities providing detection and response, such as increasing cybersecurity visibility into more diverse network types supporting the grid environment (i.e., Long Term Evolution (LTE) cellular);
- Industrial Control Systems (ICS) Threat & Asset Visibility and Information Protection capabilities: Vulnerability Management, Boundary Defense, Access Control, System Response, Device Management, and Malware Protection which all provide more granular examination of ICS-specific and proprietary protocols and applications;
- Cybersecurity Lab/destructive test environment to evaluate the hardware and software security controls of equipment, that can interface with grid-supporting devices, to limit the risk of supply chain-based attacks against manufacturers;
- Grid Data Center upgrade/replace existing tools to support existing and new capabilities of cybersecurity technology, such as firewalls, proxies, and network communication equipment that SCE currently utilizes; and
- Grid Data Center capacity/technology enhancements to increase the amount of storage, computing capability, and network throughput that upgraded and new tooling will require

The Grid Modernization program requires upgrades and replacements of legacy network, communication, and computing systems to maintain the cybersecurity posture needed for SCE to continue to operate and provide new capabilities for customers. For example, the Energy Management System (EMS) is a foundational service operated by the Grid Control Center (GCC). The GCC monitors and controls the bulk power system 24/7, using SCE's EMS. As the hardware and software that make up the EMS system continue to age, the risk for failures which result in production issues increase as well. SCE Cybersecurity will support a project to refresh the aging hardware and software components of the EMS system to maintain system availability, performance, and security.

Lastly, SCE's Grid Modernization Communications system, known as NetComm,[75] is over 20 years old and no longer sufficient to meet SCE's future needs for bandwidth and latency. Additionally, the ability to apply sufficient cybersecurity controls to offset increasing cybersecurity risks is strained within the existing system. SCE plans to substantially upgrade the current NetComm system within this GRC period, requiring cybersecurity architectural design, engineering, testing, and monitoring. Grid Modernization continues development of the Field Area Network that currently includes the NetComm system and new generations of communication technology to control and receive information from grid assets, which enhances the underlying cybersecurity capabilities of NetComm.

**2. Need for Activity**

SCE's Grid Modernization Program is vital for achieving California's 2045 decarbonization mandate. To achieve these objectives the grid support infrastructure must accommodate significantly greater complexity of operations as field assets increase in number and new sources of renewable energy are monitored and controlled. As a greater percentage of California's energy consumption migrates from carbon-based sources such as gasoline and diesel, to renewable sources such as solar and wind, any power outages can disproportionally impact our customers' quality of life.[76] Distributed power generation, energy storage, and increased electrical power consumption from electric vehicle charging all depend on a smarter, more agile, more resilient, and cyber-hardened electrical grid. As society's dependence on the electric grid increases, the targeting of SCE's systems and infrastructure by criminal organizations, nation states, and ideological zealots will also increase.

With these advances, cybersecurity will play a critical role in enabling and operating these new capabilities safely, ensuring reliable service to our customers.

The modernized grid will be very different from today's electrical grid. Large-scale distributed generation, battery storage, and microgrids, as a few examples, will drive exponential growth in data consumption and processing. SCE's Grid Modernization cybersecurity program will have to

---

[75] *See* SCE-02, Vol. 06, Grid Modernization, for a detailed discussion of the NetComm project. Note that the forecast for this project is included in the Grid Modernization volume, however, Cybersecurity will support activities discussed such as architectural design, engineering, testing, and monitoring.

[76] Note that SCE does not assert that the migration will result in power outages, but rather that power outages will be more impactful to our customers because of this migration. For example, whereas people today can still use gas and diesel to power their vehicles if there is a significant outage, in the future they might not be able to since we are not diversifying power sources. This migration also makes SCE's electric grid more attractive to people wishing harm, which is why cybersecurity will be more critical than ever in the coming years.

accommodate network connections to devices and systems which are owned and controlled by third parties, making zero-trust architectures, improved visibility, and improved security controls essential for SCE's Network Perimeter Defense. Data integrity and availability will be critical for grid stability. While SCE will not achieve these capabilities at full scale during this GRC period, lab work to develop and test these future grid capabilities, new IT system architectures, and enhanced Distributed Energy Resource for substation automation schemes will all require cybersecurity visibility and controls to protect the associated systems and architectures.

**3. RAMP Integration**

**a) O&M**

The GRC estimate for Grid Modernization Cybersecurity O&M in test year 2025 has increased beyond the RAMP estimate primarily due to additional grid modernization and engineering which will include: 1) Core cybersecurity infrastructure for Grid datacenters; 2) Threat modeling and vulnerability management; 3) Grid Lab networks for technology advancement and testing; 4) Field area network and remote sites monitoring and protection; 5) Industrial Control Systems security; 6) Security Operations; 7) Active and Passive testing; 8) Third party supplier risk mitigations; 9) Analytics and deep learning Internet of Things (IoT)[77] telemetry that collects a large amount of data from grid assets to use for modeling to increase efficiency of energy usage and distribution; 10) Cloud adoption for data sharing with external entities; and 11) Operational Technology - Zero Trust Architecture. As noted elsewhere in this testimony, Grid Modernization is essential for achieving the renewable energy objectives of California's 2045 initiative, including a goal of 60% renewable energy by 2030. As the planning to meet these renewable mandates has become clearer in the time between the 2022 RAMP filing and this GRC filing, so too has the need for additional cybersecurity support to Grid Modernization. The O&M increase in 2025 GRC over the 2025 RAMP estimate accounts for additional internal and contracted resources. These resources will support cybersecurity architecture, design, buildout, threat modeling, vulnerability management, and additional monitoring and protection of all aspects of the expanded and modernized grid infrastructure and third-party programs. RSE values

---

[77] "The Internet of Things (IoT) describes the network of physical objects – 'things'- that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025." Oracle, IoT topics, *available at* https://www.oracle.com/internet-of-things/what-is-iot.

changed based on moving to the weighted average cost of capital (WACC) for future cost discounting and updating of the financial forecasts.

***Table II-10***
***RAMP vs. GRC O&M Forecast Comparison***
*(Nominal $000)*[78]
***Risk Spend Efficiencies Comparison***[79]

| RAMP Risk | RAMP ID | RAMP Control / Mitigation Name | Filing | 2022 | 2023 | 2024 | 2025 | 2025 - 2028 RSE |
|---|---|---|---|---|---|---|---|---|
| CyberAttack | C5 | Grid Modernization Cybersecurity | RAMP | $617 | $621 | $626 | $629 | 100 |
| | | | GRC | $762 | $612 | $593 | $4,914 | 48 |
| | | | Variance | $145 | ($10) | ($33) | $4,285 | (52) |

**b) Capital**

Similar to the variances noted within the O&M section above, the Capital estimate for this GRC filing is higher than the RAMP estimate primarily due to increases in the following: 1) Network, Endpoint, Application, and Data security devices and platforms; 2) Advanced threat detection and vulnerability management tools; 3) Lab networks for security research and development, testing, and capability demonstrations; 4) Field area network/remote sites monitoring and protection; 5) IoT device certificates; 6) OT network sensors for threat monitoring and detection; 7) security testing and isolated infrastructure where testing can be performed without impacting normal operations; 8) Vendor threat detection capabilities; 9) Telemetry for IoT logs, central data repository, and machine learning technologies; 10) Cloud gateway, head-end components, and data aggregators; 11) Client authentication certificates; and 12) Telecom security equipment.

The higher cybersecurity capital cost estimates for 2025 through 2028 are driven by additional cybersecurity infrastructure and tools needed to protect Grid datacenters, to gain network visibility to monitor field assets for anomalous behavior, and to harden OT assets and networks to protect a significantly larger number of assets that are more diverse in type, and more technologically capable, than SCE's current environment. SCE's cybersecurity team must also plan for future threats

---

78 Refer to WP SCE-04, Vol. 03, pp. 29 – 48, Cyber RAMP Integration.

79 The RSE values are inconclusive of the total O&M and Capital Expenditures for the controls across all applicable GRC activities. SCE cannot readily parse out the RSE by O&M vs. Capital and by the GRC activities and by the individual GRC activity.

and vulnerabilities by implementing Zero Trust technologies and machine learning[80] for IoT-related security. RSE values changed based on moving to the weighted average cost of capital (WACC) for future cost discounting and updating the financial forecasts.

***Table II-11***
***RAMP vs. GRC Capital Forecast Comparison***
*(Nominal $000)*[81]
***Risk Spend Efficiencies Comparison***[82]

| RAMP Risk | RAMP ID | RAMP Control / Mitigation Name | Filing | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 | 2025 - 2028 Total Spend |
|---|---|---|---|---|---|---|---|---|---|---|---|
| CyberAttack | C5 | Grid Modernization Cybersecurity | RAMP | $28,934 | $36,426 | $37,440 | $36,348 | $35,675 | $29,029 | $23,475 | $124,527 |
| | | | GRC | $29,018 | $41,971 | $43,694 | $69,227 | $72,385 | $63,969 | $55,527 | $261,107 |
| | | | *Variance* | $84 | $5,545 | $6,254 | $32,879 | $36,710 | $34,940 | $32,052 | $136,580 |

## 4. Comparison of Authorized 2021 to Recorded

### a) O&M

In the 2021 GRC test year, the Commission authorized $0.683 million for Grid Modernization Cybersecurity O&M. SCE recorded expenses of $0.657 million in the 2021 test year. The variance of $26,000 is due to contractual savings on professional services.

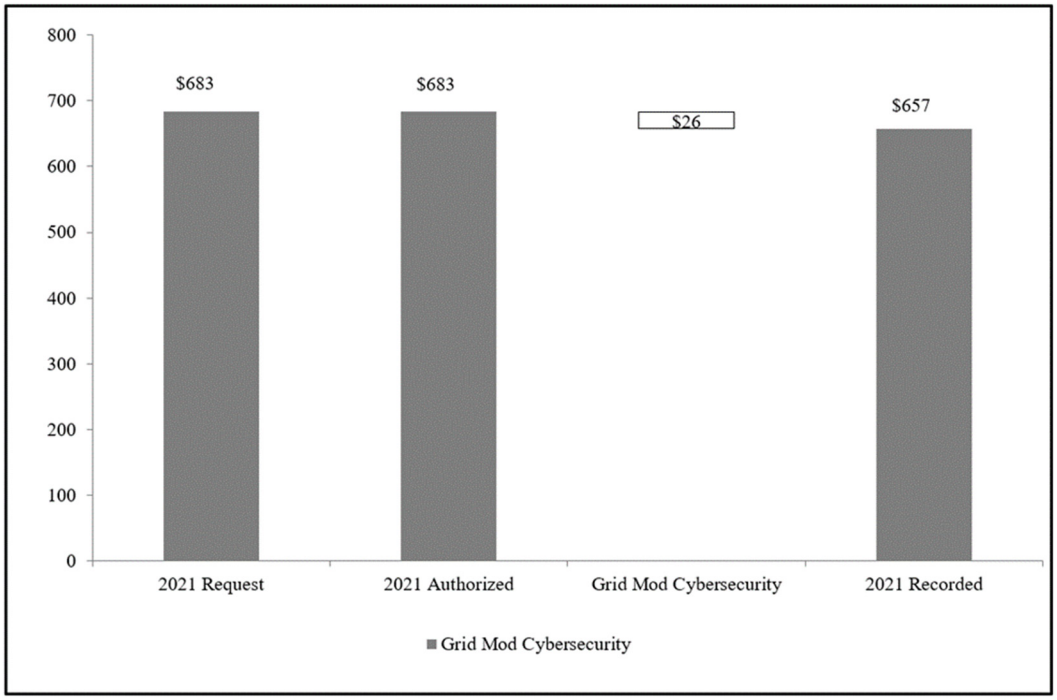
---

[80] Machine learning refers to computer systems that learn and adapt to identify patterns and deduce outcomes in a manner similar to human logic, but on a much larger scale and faster pace than human capabilities. As it relates to cybersecurity, machine learning can detect patterns of device or network activity where individual events may seem benign, but in a sequence or in context of other activities may constitute a security breach.

[81] Refer to WP SCE-04, Vol. 03, pp. 29 – 48, Cyber RAMP Integration.

[82] The RSE values are inconclusive of the total O&M and Capital Expenditures for the controls across all applicable GRC activities. SCE cannot readily parse out the RSE by O&M vs. Capital and by the GRC activities and by the individual GRC activity.

***Figure II-14***
***Grid Modernization Cybersecurity***[83]
***Comparison of 2021 Authorized versus Recorded O&M Expenses***
*(Constant 2022 $000)*

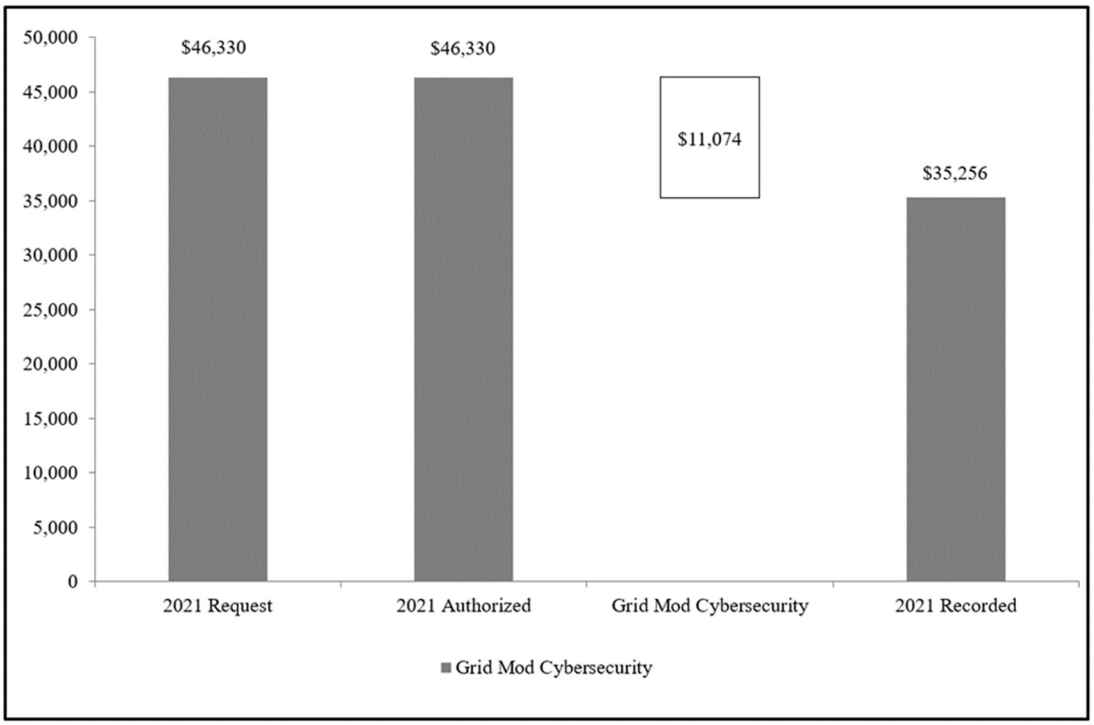



**b) Capital**

In the 2021 GRC test year, the Commission authorized $46.330 million for Grid Modernization Cybersecurity. SCE recorded expenditures of $35.256 million in the 2021 test year, which is $11.074 million less than authorized. Cybersecurity variances arose from a delay in the Grid Modernization Program; this work was deferred from 2021 to 2023 and 2024, still within the 2021 GRC period.

[83] *See* WP SCE-07, Vol. 01, Authorized vs. Recorded.

***Figure II-15***
***Grid Modernization Cybersecurity***[84]
***Comparison of 2021 Authorized versus Recorded Capital Expenditures***
*(Nominal $000)*




## 5. Scope & Forecast Analysis

### a) Historical Variance Analysis

#### (1) Labor

***Table II-12***
***Grid Modernization Cybersecurity O&M Expenses***[85]
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $156 | $216 | $318 | $127 | $105 | $115 | $75 | $352 |
| *Non-Labor* | $3,446 | $892 | $269 | $530 | $657 | $481 | $491 | $4,135 |
| *Other* | | | | | | | | |
| Total Expenses | **$3,602** | **$1,108** | **$586** | **$657** | **$762** | **$596** | **$567** | **$4,487** |

As shown in Table II-12, low levels of recorded labor costs were incurred from 2018 to 2022 as Grid Modernization Cybersecurity was in its planning and scoping stage. In 2020, there was a slight increase as more architecture and engineering resources were onboarded to provide

their expertise in cybersecurity engineering, architecture, system design, governance, and risk functions at this stage of the program. In 2020-2021, and again in 2021-2022, recorded labor decreased because architecture and engineering resources shifted their work from O&M projects to capital projects.

**(2) Non-Labor**

***Table II-13***
***Grid Modernization Cybersecurity O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $156 | $216 | $318 | $127 | $105 | $115 | $75 | $352 |
| *Non-Labor* | $3,446 | $892 | $269 | $530 | $657 | $481 | $491 | $4,135 |
| *Other* | | | | | | | | |
| Total Expenses | **$3,602** | **$1,108** | **$586** | **$657** | **$762** | **$596** | **$567** | **$4,487** |

In 2018, the non-labor costs reflect a one-time increase of $2.5 million due to an accounting change causing hardware maintenance costs to be moved from Capital to O&M consistent with SCE accounting practices, resulting in certain Grid Modernization Cybersecurity non-labor costs being moved from capital to O&M.[86]

In 2019, the accounting change did not take place, so the spend reflected purely the activities done within this time period. Non-labor costs for Grid Modernization Cybersecurity include costs for training and conferences, training travel expenses, and conducting onsite training support on the operations of the cybersecurity network boundary defense and industrial controls system security tools and technologies. As reflected above, SCE began incurring non-labor expenses in 2018 as outside resources are utilized to perform architecture evaluations and build requirements definitions as part of the planning and scoping effort.

In 2020, SCE experienced the global impact of the COVID-19 pandemic. Therefore, SCE made necessary adjustments to normal operations and practices in an effort to mitigate the risk of COVID-19 transmittal and spread, and in order to comply with COVID-driven governmental

---

[84] *See* WP SCE-07, Vol. 01, Authorized vs. Recorded.

[85] Refer to WP SCE-04, Vol. 03, pp. 81 – 88, Grid Modernization Cybersecurity – Standard Workpapers.

[86] Please refer to SCE-07, Vol. 01 for SCE's accounting practices and the 2021 GRC's SCE-04, Vol. 03 Cybersecurity testimony where this accounting change is also mentioned.

directives and guidance. Some of these adjustments by SCE impacted to a degree the scope of activities related to business travel, attending job-related or industry-related conferences, or engaging in normal levels of in-person training. As a result of the protocols that we necessarily adopted during the pandemic, the recorded expenses for this activity in 2020 decreased significantly. In 2021 and 2022, the increases were related to online training modules that were purchased to offset the training gaps experienced during COVID-19.

**(3) Capital**

***Table II-14***
***Grid Modernization Cybersecurity Capital Expenditures***[87]
***2018-2022 Recorded / 2023-2028 Forecast***
*(Nominal $000)*

| | Recorded | | | | | Forecast | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 |
| Grid Mod Cybersecurity | $21,267 | $26,136 | $22,892 | $35,256 | $29,018 | $41,971 | $43,694 | $69,227 | $72,385 | $63,969 | $55,527 |
| **Totals** | **$21,267** | **$26,136** | **$22,892** | **$35,256** | **$29,018** | **$41,971** | **$43,694** | **$69,227** | **$72,385** | **$63,969** | **$55,527** |

Consistent with SCE's prior GRCs, the volume and complexity of application refreshes varying from year to year is driven by application obsolescence, which drove the fluctuations from 2018-2022.

Capital costs increased from $21.267 million to $26.136 million between 2018 to 2019. This is mostly attributable to the volume of foundational tools and complexity of the refreshes performed within that year.

In 2020, capital spend decreased to $22.892 million due to less refreshes on legacy technologies being performed.

Capital increased from $22.892 million in 2020 to $35.256 million in 2021 due to investments in remote tools to accommodate the Grid security advancement necessary to support remote work and increases in refreshes to legacy technologies.

Finally, capital spend decreased from 2021 to 2022 due to the lower volume of foundational tools and complexity of the refreshes performed within those years.

---

87 Refer to WP SCE-04, Vol. 03, pp. 81 – 88, Grid Modernization Cybersecurity – Standard Workpapers.

**b) Forecast**

**(1) Labor**

***Table II-15***
***Grid Modernization Cybersecurity O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $156 | $216 | $318 | $127 | $105 | $115 | $75 | $352 |
| *Non-Labor* | $3,446 | $892 | $269 | $530 | $657 | $481 | $491 | $4,135 |
| *Other* | | | | | | | | |
| Total Expenses | **$3,602** | **$1,108** | **$586** | **$657** | **$762** | **$596** | **$567** | **$4,487** |

Grid Modernization Cybersecurity forecasts $352 million for Test Year 2025 for Labor. This forecast utilizes an itemized forecasting methodology and reflects an increase from prior years due to the significant increase in cybersecurity engineering and design work in support of grid expansion and modernization necessary to realize California's 2045 mandate. This increase includes costs associated with developing new communications pathways to support existing grid traffic, as well as enabling SCE to grow its portfolio of grid security and reliability technologies such as increasing the frequency of data polled from substations and field devices to better model current capacity and load, along with forecasting predicted demand based on weather and other outside factors. The creation of these new communication pathways forms a foundation for new ways of enabling grid equipment communication and must be protected from unauthorized and malicious activity.

As mentioned earlier in the changing nature of SCE's grid to support increasing amounts of renewable energy, and the exponential increase in connectivity necessary for telemetry, new technologies, and increased grid automation, SCE will perform additional cybersecurity engineering and testing related to field radio updates, and Advanced Metering Infrastructure (AMI) methodology in support of the labor forecast. These activities include projects and components to increase the cybersecurity posture for the AMI and field radio environments with respect to new capabilities, such as enhancing the remote functionality of devices used to increase reliability in the distribution environment and increasing the amount of relevant information available to customers regarding usage of renewable energy, that these

systems will be performing in the upcoming years. For additional details, please see supplemental work papers.[88]

**(2) Non-Labor**

***Table II-16***
***Grid Modernization Cybersecurity O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $156 | $216 | $318 | $127 | $105 | $115 | $75 | $352 |
| *Non-Labor* | $3,446 | $892 | $269 | $530 | $657 | $481 | $491 | $4,135 |
| *Other* | | | | | | | | |
| Total Expenses | **$3,602** | **$1,108** | **$586** | **$657** | **$762** | **$596** | **$567** | **$4,487** |

SCE forecasts $4,135 million for Non-Labor O&M in test year 2025.[89] This forecast also utilizes an itemized forecasting methodology and reflects additional investments to modernize SCE's grid. To accomplish this significant undertaking, SCE will require considerable contractor engagement to address the specialties, complexities, and scale necessary to modernize the grid. The nature of these advancements requires both unique skills – which are uncommon even among experienced cybersecurity practitioners – and SCE's expert knowledge of our grid, operations, regulations, and customer needs.

As the expertise needed is only required for the duration of the effort, hiring contractors would be more appropriate than hiring full time employees, given the time-constrained nature of the work. Working under SCE's direction and supervision, contractors will support and assist with the following: 1) Core cybersecurity infrastructure for Grid datacenters; 2) Threat modeling and vulnerability management; 3) Grid Lab networks for technology advancement and testing; 4) Field area network and remote sites monitoring and protection; 5) Industrial Control Systems security; 6) Security Operations; 7) Active and Passive testing; 8) Third party supplier risk mitigations;

---

[88] Refer to WP SCE-04, Vol. 03, pp. 89 – 90, Grid Mod Cybersecurity 2023-2028 O&M Labor and Non-Labor Workpapers. Note that the forecast also incorporates an increase attributable to an adjustment to reflect certain changes made to SCE's employee compensation program. Please refer to SCE-06, Vol. 04.

[89] Calculation of normalization amount is as follows: [2025 amount of 3,819 + 2026 amount of 4,586 + 2027 amount of 4,597+ 2028 amount of 3,540] /4= the updated 2025 normalized amount of **$4,135**. Dollars are in constant and in '000.

9) Analytics and deep learning IoT telemetry; 10) Cloud adoption for data sharing with external entities; and 11) Operational Technology - Zero Trust Architecture.

As the basis for its forecast, SCE utilized an itemized methodology to properly reflect the impact of those initiatives. Some of the skills and experience necessary to securely design and deploy this new technology are provided by subject matter experts with extensive backgrounds on the potential impacts to normal utility operations as well as how to prevent and rapidly respond to situations or incidents arising from the use of such technology. For example, increasing the amount of data that is sent from connected grid devices allows SCE to improve modeling of current and future grid conditions. To increase that data, systems which previously were not network-connected are being updated and connected into field area networks, which increases risk of unauthorized access for these devices, as well as risk to the field area network itself from these devices if they are compromised. Once the grid systems are connected, the integrity of the data must be assured so that decisions made to increase efficiency and reliability are based on factual information. Due to the rapidly updating technology ecosystem of connected devices and IoT, SCE must be aware of the risks and defensive actions needed to protect these systems. Each of these connections must be evaluated before implementation, during execution, and after it is commissioned for normal operations. These subject matter experts include both vendor-specific and industry-focused resources on leading-edge and cutting-edge technologies that would be impractical for SCE to have as full-time employees. For additional details, please see supplemental work papers.[90]

**(3) Capital**

***Table II-17***
***Grid Modernization Cybersecurity Capital Expenditures***
***2018-2022 Recorded / 2023-2028 Forecast***
*(Nominal $000)*

| | Recorded | | | | | Forecast | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 |
| Grid Mod Cybersecurity | $21,267 | $26,136 | $22,892 | $35,256 | $29,018 | $41,971 | $43,694 | $69,227 | $72,385 | $63,969 | $55,527 |
| **Totals** | **$21,267** | **$26,136** | **$22,892** | **$35,256** | **$29,018** | **$41,971** | **$43,694** | **$69,227** | **$72,385** | **$63,969** | **$55,527** |

Grid Modernization Cybersecurity's capital expenditures forecast for 2023-2028 is $346.773 million. The capital forecast is also driven by SCE's initiatives to build a more

[90] Refer to WP SCE-04. Vol. 03, pp. 89 – 90, Grid Mod Cybersecurity 2023-2028 O&M Labor and Non-Labor Workpapers.

flexible and capable grid necessary to meet California's 2045 mandate. The twelve areas enumerated in O&M non-labor above all require capital investments.

Examples of these Capital investments include: 1) Network, Endpoint, Application, and Data security devices and platforms to upgrade existing systems, and to replace outdated systems to ensure that multiple layers of protection can be applied at connections, including communication, signature-based anti-virus/malware, behavioral analysis, allow and disallow listing of programs, and ensuring that sensitive data is encrypted within the environment; 2) Advanced threat detection and vulnerability management tools which do not rely solely on signature-based updates and can dynamically evaluate network traffic and behavior to halt and alert on suspicious behavior; 3) Lab networks for security research and development, testing, and capability demonstrations to allow for testing and training methods which could expose systems to unknown cybersecurity threats through experimental application and detailed investigation to be evaluated in a non-production environment; 4) Field area network/Remote sites monitoring and protection to extend network and application monitoring and alerting closer to the SCE customers for more reliable information and alerting; 5) IoT device certificates to protect the confidentiality and integrity of equipment status, operating parameters, and data generated by field equipment; 6) OT network sensors for threat monitoring and detection by performing deep-packet inspection of proprietary and industry-specific application traffic and network protocols; 7) Security testing and sandboxing infrastructure which allows for internal and third party cybersecurity testing and evaluation to be performed at a lower risk for disrupting SCE infrastructure; 8) Vendor threat detection capabilities to provide early warnings and increase awareness of cybersecurity threats targeted at electric utilities; 9) Telemetry for IoT logs, central data repositories, and machine learning technologies to develop machine learning models to increase efficiency of grid operations, maintenance, and response to issues; 10) Cloud gateway, head-end components, and data aggregators that provide connections for outside entities to securely exchange relevant and necessary information to make decisions on electric grid operations; 11) Client authentication certificates which reduce the likelihood that an attacker could spoof the identities of SCE system users and gain unauthorized access; and 12) Telecom security equipment to enable additional security features provided by newer generation communication networks, such as LTE.

The capital investments needed are focused on the acquisition of hardware and software necessary to augment the SCE environment to support the areas mentioned in the O&M

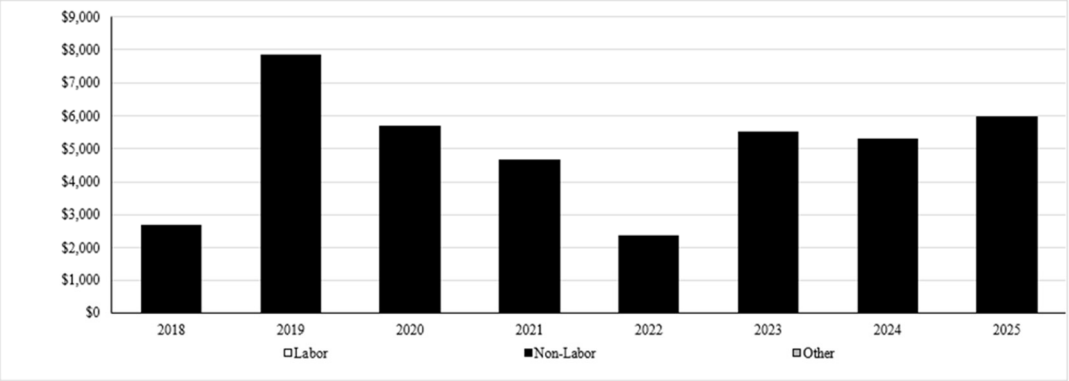
non-labor section above.[91] As these are new technologies and capabilities, they require infrastructure and control equipment to provide these functions. Examples of these investments include Deep Packet Inspection technology that is capable of interpreting Industrial Control System (ICS) specific protocols and services. In order to provide more real-time information on the status of the electricity grid, there has been rapid growth in the use of IoT devices, which provide large amounts of data. IoT systems offer a unique challenge for utilities as they require access to the internet in order to operate, whereas most utility systems are designed to operate without the internet or in a disconnected state. The methods for securing these devices and protecting the privacy of customer information require new types of security technology that are relatively new to the market and have higher costs. Many of these technologies also utilize Machine-learning features to build models that can be utilized to automate alerting of non-typical behavior which can greatly reduce the amount of time needed to identify issues. Machine-learning systems require a large amount of data storage and computing power in order to generate these models, both of which increase costs of development and operations, but which are required to ensure the security of our systems and information.

**D. Software License & Maintenance**

Figure II-16 shows 2018-2022 recorded costs and Test Year 2025 forecast for the Software License & Maintenance activity.

[91] Refer to WP SCE-04, Vol. 03, pp. 91 – 93, Grid Mod Cybersecurity Capital 2023-2028 Workpapers.

***Figure II-16***
***Software License & Maintenance O&M Expenses***[92]
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*




| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $4 | $10 | $13 | $7 | $6 | | | |
| *Non-Labor* | $2,668 | $7,830 | $5,681 | $4,639 | $2,344 | $5,517 | $5,301 | $5,950 |
| *Other* | | | | | | | | |
| Total Expenses | **$2,673** | **$7,840** | **$5,695** | **$4,647** | **$2,351** | **$5,517** | **$5,301** | **$5,950** |

## 1. Work Description

The Cybersecurity Software Licenses & Maintenances activity includes the costs of licenses and maintenance agreements to maintain SCE's cybersecurity hardware and software assets.

These costs include software support agreements that give SCE access to break/fix support, service patches, software updates, and upgrades of all kinds for a large variety of cybersecurity software products used by SCE. The secure operation and maintenance of these applications is vital and the patches and updates from vendors are needed to address security, operational defects and operating system compatibility and improve performance.

The regular introduction of new tools or projects can result in year-to-year variances in the software spend. New software implementations normally come with five years of pre-paid, capitalized licensing and maintenance costs. After five years, the maintenance costs are treated as O&M. The number and size of license renewals vary from year to year depending on the year of software implementation.

[92] Refer to WP SCE-04, Vol. 03, pp. 94 – 100, Cybersecurity Software License and Maintenance – Standard Workpapers.

## 2. Need for Activity

Cybersecurity attacks are constantly changing and require frequent updates and changes in defensive technology to adjust. Ensuring that cybersecurity tools are up to date requires investment in the licensing and maintenance for adequate coverage across the spectrum of adversarial activity.

Cybersecurity presents an ever-evolving challenge to SCE. The threat of cyberattacks is growing; attacks are continually becoming more frequent and more sophisticated. Our grid is evolving and incorporating communication and operating technology that enable us to respond faster, operate our system more efficiently and reliably, and incorporate distributed energy resources at a greater level. But more reliance on advanced technology to operate and communicate necessarily increases the risk of cyberattacks, and greater potential consequences if a cyberattack is successful.

SCE needs the latest tools to protect against cyber threats. Such threats include malicious intrusion by hackers or insiders and the proliferation of various forms of attacks through malware, denial of service attacks and viruses. These threats can affect the ability to provide reliable generation and delivery of electric power. Without these tools, SCE would be vulnerable to harmful infiltration. Regular renewal of vendor support and maintenance for our software is needed to secure vendor availability to respond in a timely fashion when critical systems experience outages or system failures.

The most common method of remediating cybersecurity vulnerabilities is through software patching. The Cybersecurity and Infrastructure Security Agency (CISA) maintains a catalog of more than 18,300 exploitable Common Vulnerabilities and Exposures (CVEs) with hundreds more added each year.[93] These vulnerabilities frequently require software upgrades and patching to prevent attackers from exploiting them. Without software license and maintenance agreements, SCE is unable to patch software and maintain its security. Absent implementation of critical security patches, the security of customer data and critical system infrastructure would be placed at significant risk. As new threats arise that are not addressed by the existing software and hardware in use, these support contracts allow SCE to get access to development and engineering resources to generate appropriate countermeasures.

---

[93] Samantha Schwartz, *CISA Overhauls Vulnerability Management, Focuses on CVEs Under Active Exploit,* CYBERSECURITY DIVE, Nov. 3, 2021, *available at* https://www.cybersecuritydive.com/news/CISA-vulnerability-patch-directive-CVE-catalog/609393/.

### 3. RAMP Integration

#### a) O&M

As shown in Table II-18, the changes reflected in these forecasts are not material and are a reflection of normal refinements through our forecasting process. RSE values changed based on moving to the weighted average cost of capital (WACC) for future cost discounting and updates to the financial forecasts.

***Table II-18***
***RAMP vs. GRC O&M Forecast Comparison***
*(Nominal $000)*[94]
***Risk Spend Efficiencies Comparison***[95]

| RAMP Risk | RAMP ID | RAMP Control / Mitigation Name | Filing | 2022 | 2023 | 2024 | 2025 | 2025 - 2028 RSE |
|---|---|---|---|---|---|---|---|---|
| CyberAttack | C1 | Perimeter Defense | RAMP | $1,043 | $2,006 | $2,006 | $2,181 | 351 |
| | | | GRC | $877 | $2,049 | $2,008 | $2,346 | 322 |
| | | | Variance | ($166) | $42 | $1 | $165 | (29) |
| CyberAttack | C2 | Interior Protection | RAMP | $596 | $1,147 | $1,147 | $1,234 | 477 |
| | | | GRC | $488 | $1,152 | $1,129 | $1,308 | 423 |
| | | | Variance | ($108) | $5 | ($18) | $74 | (54) |
| CyberAttack | C3 | Data Protection | RAMP | $596 | $1,147 | $1,147 | $1,147 | 460 |
| | | | GRC | $397 | $1,020 | $1,000 | $1,081 | 412 |
| | | | Variance | ($199) | ($126) | ($147) | ($65) | (48) |
| CyberAttack | C4 | SCADA Cybersecurity | RAMP | $149 | $287 | $287 | $287 | 796 |
| | | | GRC | $99 | $255 | $250 | $270 | 706 |
| | | | Variance | ($50) | ($32) | ($37) | ($16) | (90) |
| CyberAttack | C5 | Grid Modernization Cybersecurity | RAMP | $596 | $1,147 | $1,147 | $1,234 | 100 |
| | | | GRC | $488 | $1,152 | $1,129 | $1,308 | 48 |
| | | | Variance | ($108) | $5 | ($18) | $74 | (52) |

### 4. Comparison of Authorized 2021 to Recorded

#### a) O&M

In the 2021 GRC Test Year, SCE was authorized $6.304 million in O&M expenses for Software License & Maintenance. This work activity recorded O&M expenditures of

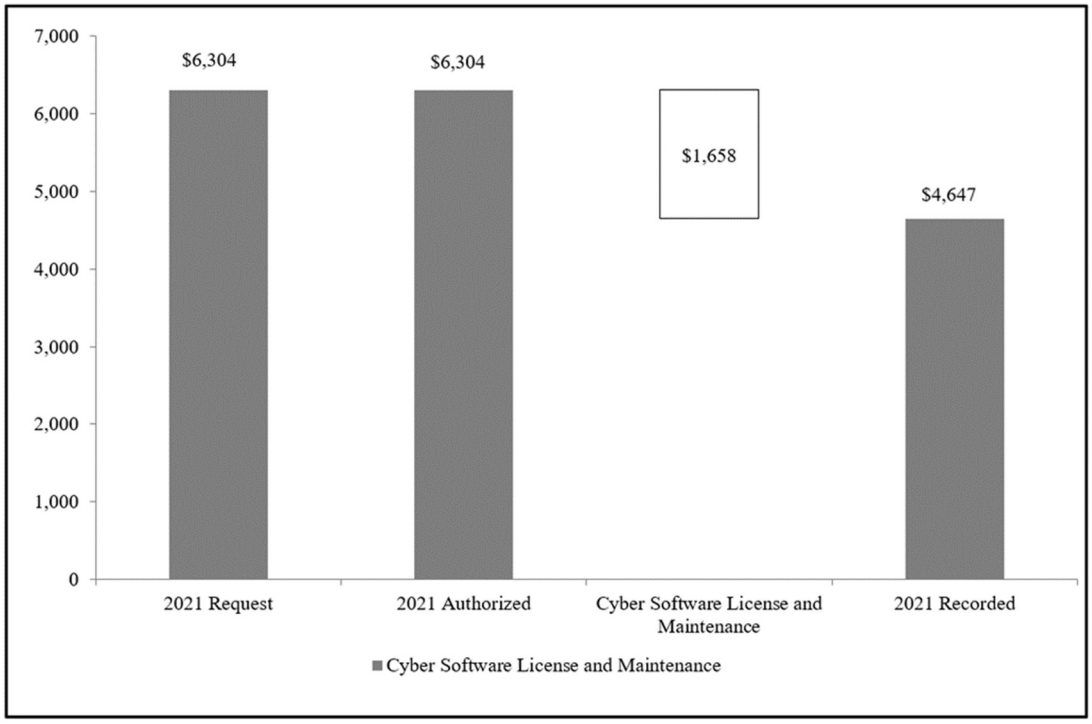
---

94 Refer to WP SCE-04, Vol. 03, pp. 29 – 48, Cyber RAMP Integration.

95 The RSE values are inconclusive of the total O&M and Capital Expenditures for the controls across all applicable GRC activities. SCE cannot readily parse out the RSE by O&M vs. Capital and by the GRC activities and by the individual GRC activity.

$4.647 million, which was $1.658 million below authorized. This decrease in spending compared to authorized was primarily due to savings from various license negotiations and fewer licenses purchased than originally forecasted.

***Figure II-17***
***Software License & Maintenance***[96]
***Comparison of 2021 Authorized versus Recorded O&M Expenses***
*(Constant 2022 $000)*




[96] *See* WP SCE-07, Vol. 01, Authorized vs. Recorded.

## 5. Scope & Forecast Analysis

### a) Historical Variance Analysis

#### (1) Labor

***Table II-19***
***Software License & Maintenance O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $4 | $10 | $13 | $7 | $6 | | | |
| *Non-Labor* | $2,668 | $7,830 | $5,681 | $4,639 | $2,344 | $5,517 | $5,301 | $5,950 |
| *Other* | | | | | | | | |
| Total Expenses | **$2,673** | **$7,840** | **$5,695** | **$4,647** | **$2,351** | **$5,517** | **$5,301** | **$5,950** |

Table II-19 reflects minimal labor expenses from supply chain to process purchase orders for cybersecurity software licenses and maintenance.

#### (2) Non-Labor

***Table II-20***
***Software License & Maintenance O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $4 | $10 | $13 | $7 | $6 | | | |
| *Non-Labor* | $2,668 | $7,830 | $5,681 | $4,639 | $2,344 | $5,517 | $5,301 | $5,950 |
| *Other* | | | | | | | | |
| Total Expenses | **$2,673** | **$7,840** | **$5,695** | **$4,647** | **$2,351** | **$5,517** | **$5,301** | **$5,950** |

Non-labor costs for this activity vary from 2018 to 2022 because the volume of support, maintenance, renewals, and upgrades needed fluctuate from year to year and are based on the negotiated terms of multiple software and license agreements. SCE would normally capitalize initial license purchases with five years of maintenance, and the higher spend in 2019-2021 reflected expanding scope as capitalized maintenance from grid modernization shifted to yearly O&M software renewals. The decrease in 2022 reflected the decommissioning of certain licenses as new capital acquisitions were made.

**b) Forecast**

**(1) Labor**

***Table II-21***
***Software License & Maintenance O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $4 | $10 | $13 | $7 | $6 | | | |
| *Non-Labor* | $2,668 | $7,830 | $5,681 | $4,639 | $2,344 | $5,517 | $5,301 | $5,950 |
| *Other* | | | | | | | | |
| Total Expenses | **$2,673** | **$7,840** | **$5,695** | **$4,647** | **$2,351** | **$5,517** | **$5,301** | **$5,950** |

SCE does not forecast any labor costs in for Software License & Maintenance in Test Year 2025.

**(2) Non-Labor**

***Table II-22***
***Software License & Maintenance O&M Expenses***
***2018-2022 Recorded / 2023-2025 Forecast***
*(Constant 2022 $000)*

| | Recorded | | | | | Forecast | | |
|---|---|---|---|---|---|---|---|---|
| | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** | **2025** |
| *Labor* | $4 | $10 | $13 | $7 | $6 | | | |
| *Non-Labor* | $2,668 | $7,830 | $5,681 | $4,639 | $2,344 | $5,517 | $5,301 | $5,950 |
| *Other* | | | | | | | | |
| Total Expenses | **$2,673** | **$7,840** | **$5,695** | **$4,647** | **$2,351** | **$5,517** | **$5,301** | **$5,950** |

SCE's non-labor forecast for 2025 is $5.950 million.

The Cybersecurity Software License & Maintenance activity provides the essential support to securely operate and maintain the reliability and performance of critical tools employed for our cybersecurity strategy. These tools are utilized for all Cybersecurity Programs. For example, firewall technology utilizes licenses and software features to enable specific security controls, such as deep packet inspection. Absent this license and software, the security control would be disabled or prevented from receiving future updates. This would severely degrade the capability of this Perimeter Defense control and reduce the ability to prevent or mitigate cyber-attacks.

The forecast is based on the costs which factor in both continual increases in cost for these types of technologies and additional purchases needed to support growth. To establish

this forecast, SCE utilized an itemized list of software and licenses aligned with what has been identified in RAMP to support the grid. In some cases, these technology solutions may be upgraded or augmented to operate more efficiently and improve the security posture of SCE. Please refer to the workpaper which outlines the lifecycle for these tools and upgrades and discusses the drivers for the timing of the refresh and associated costs that form the basis for the forecast.[97]

[97] Refer to WP SCE-04, Vol. 03, pp. 101 – 105, Cyber Software License and Maintenance Workpaper.