March 30, 2018

Alice Stebbins
Executive Director
California Public Utilities Commission
505 Van Ness Avenue
San Francisco, CA 94012-3298

Re: California Energy Systems for the 21st Century (CES-21) Annual Report - 2017

Dear Ms. Stebbins:

The 2017 CES-21 annual report is submitted by San Diego Gas & Electric Company (SDG&E), on behalf of itself, Pacific Gas & Electric Company (PG&E) and Southern California Edison Company (SCE), pursuant to Ordering Paragraph 21 of Commission Decision 14-03-029.

This report provides information on the operations of the CES-21 program, including projects funded, results of research, efforts made to involve additional third parties, and intellectual property that results from the research.

Please contact Tim Lyons at TLyons@semprautilities.com, Leslie Arnold at LEA6@pge.com, or John Minnicucci at John.Minnicucci@sce.com regarding any questions about this report. Thank you.

Attachment

Copies to: Melicia Charles, CPUC Energy Division
David Huang, CPUC Energy Division
Leslie Almond, PG&E Regulatory
Dan Gilani, PG&E
John Minnicucci, SCE Regulatory
Joy Weed, SCE
Tim Lyons, SDG&E Regulatory
Corey McClelland, SDG&E

California Energy Systems for the 21st Century (CES-21) Program

2017 Annual Report

March 31, 2018

Table of Contents

1. Executive Summary

a. Overview of CES-21 Program and Plan Highlights

The California Energy Systems for the 21st Century (CES-21) Program is a public-private collaborative research and development program between the California Joint Utilities[1] and Lawrence Livermore National Laboratory (LLNL). The purpose of this annual report is to provide the California Public Utilities Commission (CPUC or Commission) with a summary of the 2017 progress of the CES-21 Program[2].

The CES-21 Program is designed to research solutions for the medium- and far-term challenges of a fast-evolving energy marketplace. The program is comprised of two projects:

1. **Cybersecurity Project:** Pursues research in next-generation areas of Industrial Control Systems (ICS) cybersecurity. This research falls into three major work streams:

    - Developing a *Modeling / Simulation Platform* to simulate threat and response scenarios. The simulation engine will enable virtual testing of remediations at scale to identify potential negative externalities. It also enables destructive tests to be performed without endangering actual equipment. The simulation engine represents the merging of two types of modeling systems: network data systems and grid configuration power flow models. Each of these categories has well-developed examples, but they are not typically combined. Each development cycle is designed to build on the functionality of the previous cycle, with the end goal of being able to model a mid-sized grid environment and the data communications which control it.
    - Establishing a *Physical Test Bed* to evaluate threats on actual substation equipment. This will allow testing of vulnerabilities and potential remediations using real-world equipment, but in a contained sandbox environment. This will also allow equipment response assumptions from the simulation platform to be cross-checked against real devices.
    - Compiling an *Automated Response Research Package* to support the industry's evolution towards Machine to Machine Automated Threat Response (MMATR) and other next-generation security techniques. The Indicator Remediation Language (IRL) research has produced standardization of an indicator encoding language that has been adopted by the European Union. In addition, the Secure SCADA protocol and quantum key distribution research has broken unique capabilities demonstrated for the first time with CES-21.

    The CES-21 Cybersecurity project is comprised of a joint team of technical experts from the Joint Utilities, LLNL, other national laboratories, and contractors.

[1] Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE) and San Diego Gas & Electric Company (SDG&E), collectively the Investor Owned Utilities (IOUs) or "Joint Utilities".
[2] Per the reporting requirements detailed in CPUC Decision (D.) 14-03-029, Ordering Paragraph (OP) 21.

2. **Grid Integration - Flexibility Metrics Project:** This project worked to determine if the utilities' planning assumptions and reliability metrics were applicable under future conditions, given the goals California has adopted to increase renewable generation. This required modeling the grid under thousands of permutations of market demand, weather conditions, and infrastructure investment to simulate the impact of increased renewable penetration and market conditions on the accuracy of reliability and capacity metrics. The Grid Integration project was led by PG&E with support from SDG&E and LLNL.

b. Status of Program and 2017 Achievements

Cybersecurity Project

In 2017, the Cybersecurity project achieved research milestones across its major work streams and created research demonstrations in some of the major task areas:

1. **Simulation Engine:** In 2017, the CES-21 team completed both the third and fourth of five planned cycles of development, utilizing the modeling and simulation engine developed in prior years. The third simulation cycle focused on a grid level cyberattack that would cause system separation (islanding). It was demonstrated that cascading effects to the grid may be possible through specific combinations of attacks. The fourth simulation cycle focused on a cyberattack involving malicious adjustment of protection relay settings. This cycle helped to identify the relative importance of protecting specific relays.
2. **Physical Test Bed:** In 2017, SCE and SDG&E located equipment at Idaho National Laboratory's (INL) Physical Test Bed to create instances of their respective substations, and PG&E began the process of completing their IOU-specific equipment and configurations to be sent to INL in 2018. Having the equipment located at INL allows for comparison between the vulnerabilities and capabilities of different hardware configurations. Because each of the three IOUs implements substation devices and cybersecurity controls differently from each other, the vulnerabilities to various exploits will vary by IOU, so there is value and insight to be gained from having three separate substation instances. PG&E also placed equipment within LLNL's cyber grid test laboratory in 2017, offering more local access for LLNL, PG&E, and other team members in a setting physically close to the high-performance computing and cybersecurity analysis resources that LLNL offers. SDG&E also has a CES-21 lab at their Integrated Test Facility (IDF) which has been used for orchestration and automation of responses, quantum key distribution, and secure supervisory control and data acquisition (SCADA) protocol research among other lines of research objectives. The success of establishing these test beds allows researchers to test the CES-21 research objectives and metrics. An example is running the Indicator and Remediation Language (IRL) on actual substation equipment to determine if there are gaps in the current language set. These gaps can then be addressed by the project and submitted for acceptance by the global standards body Organization for the Advancement of Structured Information Standards (OASIS), as first successfully occurred in January 2017. Additionally, the setup of IOU equipment will allow for validation of how specific equipment is being modelled in the simulation engine. The knowledge gained at any of the CES-21 test facilities is shared amongst the team and applied as appropriate.
3. **Automated Response Research Package:** Research into advanced cyber areas continued to develop across a range of topics which in the future will be critical to automated threat response systems:

a. *Indicator and Remediation Language* (IRL): Continued development of ICS-specific extensions to the Structured Threat Information eXpression (STIX), an industry-leading indicator encoding language. These ICS-extensions were successfully submitted for inclusion in STIX 2.0 and will continue to improve future versions of the language.

b. *Exploits, Malware and Vulnerabilities (EMV):* Prototyped method, process flow and scoring of EMV.

c. *Secure SCADA Protocol for the 21st Century* (SSP21): Completed open-source specification and reference implementation of SSP21 using public key cryptography and/or shared secrets.

d. *ICS Quantum Key Distribution*: Conducted the first ever demonstration of a prototype ICS Quantum Key Distributio*n* system integrated with SSP21 using entangled photons.

e. *Quantum Key Dis*tribution and SSP-21: Demonstrated the utilization of Quantum Keys by SSP-21 implementations to secure SCADA communications.

f. *Orchestration and Automation*: Demonstrated playbooks for orchestration and automation of machine speed response and remediation of identified threats.

g. *Integration Component Architecture*: Documented a potential Integration Component Architecture across tasks, to better identify potential synergies and dependencies between tasks.

h. *Grid Operator Workshop*: Held the first Grid Operator Workshop hosted by SCE to begin socializing the research. This resulted in an excellent discussion with Operator personnel on how they monitor threats and implement remediation actions while limiting impact to grid operations. Additional Grid Operator Workshops were held at quarterly technical meetings.

4. **Program Governance and Foundational Collaboration:** The CES-21 project continued to perform outreach sessions with federal agencies and other key stakeholders to identify synergies and help ensure research non-duplication. The project continued to meet with the Joint IOU Steering Committee for direction and status updates. The Independent Advisory Committee[3] met as a group and individually with CES-21 PMs to gather knowledge and feedback from representatives and subject matter experts of federal and regulatory agencies, academia, and industry.

Grid Integration – Flexibility Metrics Project

In 2017, the Grid Integration project was successfully completed, and delivered on all of its requirements.

Specific highlights from 2017 include:

- **Modeling**
  - Completed modeling of the full Western Electricity Coordinating Council (WECC) representation, using the latest 2026 Transmission Expansion Planning Policy Committee (TEPPC) dataset, which included over 4,000 generation units and over 30 distinct electric Balancing Authorities.

[3] Including representatives from the Department of Energy, the Department of Homeland Security, NERC, and the University of California at Davis (UC Davis).

  - Simulated over 87,500 full years of system operations under various 50% Renewable Portfolio Standards (RPS) scenarios (8,760 hours each at 5-minute intervals).
  - Fully leveraged the LLNL High Performance Computing (HPC) platform developed in 2016 and the 1,000% gain in run-time efficiency, in order to complete timely analysis.
- **Sharing Results with Public** – Presented key findings and recommendations from the project on August 15, 2017 at a CPUC workshop as a part of the Integrated Resource Planning (IRP) proceeding. Provided all stakeholders opportunities to comment.
- **Providing Access to Project Results** – Filed the CES-21 Grid Integration project final report in the CPUC's IRP proceeding on September 12, 2017. Provided public access to the entire set of modeling input assumptions.

The results of the Grid Integration project are aligned with the CPUC's newly-created IRP proceeding. Some of the concepts and analytical framework developed by the Grid Integration project are being incorporated by the CPUC's modeling team in future IRP proceedings.

c. Lessons Learned

Cybersecurity Project

The following are some of the high-level lessons learned during the year for the cybersecurity project:

- **Model Development:** In the modeling and simulation field, complete models of as-built communication networks typically do not exist. The level of model fidelity required by a simulation depends highly on the analysis that is required and will affect outcomes if not properly determined up front. Therefore, it is important for SMEs and researchers to work closely to define the problem, plan the R&D project, and analyze results.
- **Information Technology (IT) and Operational Technology (OT) Integration:** IT and OT networks, equipment, staff, and processes have historically been very separate. We are seeing the convergence of these teams beginning to happen. Most of the impetus for this convergence from the IT side is being fueled by cybersecurity concerns.
- **Cybersecurity Collaboration:** There is a keen interest in industry and government agencies to collaborate with CES-21 in areas of national significance for the protection of critical infrastructure. Key lessons learned from CES-21 research have been presented at conferences where the exchange of research has helped to strengthen MMATR research.

Grid Integration

The following are some of the high-level lessons learned during the year for the Grid Integration project:

- **System Reliability:** Under the assumed resource mix studied, up to 50% RPS, the CAISO system has sufficient operating flexibility to meet demand in a reliable manner, subject to the assumption that the system operator can fully access the flexibility available including curtailments and net imports.
- **Planning Standards:** In terms of new planning standards, the CES-21 results suggest there is no need at this time to add additional flexibility-related standards for addressing reliability-related issues. Planning Reserve Margin (PRM) is still a useful metric to assess adequacy, but the Effective Load Carrying

Capability (ELCC) of all resources needs to be accurately calculated and used in the PRM calculation. It is important to simulate the full range of possible grid conditions when assessing flexibility.

- **New Metrics** – Use of new Loss of Load Expectation (LOLE) metrics – $LOLE_{INTRA\text{-}HOUR}$ and $LOLE_{MULTI\text{-}HOUR}$ allow for greater understanding of the flexibility needs and resources. How these relate to $LOLE_{CAPACITY}$ needs to be further considered.

d. Conclusion

The CES-21 program represents an unprecedented level of collaboration between the CES-21 Joint Utilities and National Labs with unique experience. The 2017 year was one in which this collaboration helped to create and deliver multiple research accomplishments which will help inform the future of our grid. The Grid Integration project has successfully completed all its required deliverables and met its overall objectives in 2017. The Cybersecurity project is producing real world research deliverables, including:

- Successful updates to a global threat indicator language to support key utility functionalities.
- A reference architecture and implementation structure for securing SCADA communications.
- A cross-functional mapping between individual tasks, documented in an integration framework.

The program participants are proud to report the accomplishments of this collaborative work through the following annual report.

2. Introduction and Overview

The purpose of this annual report is to provide the Commission with a summary of the 2017 progress of the CES-21 Program and the two projects of which it is comprised (Cybersecurity and Grid Integration). This is part of the reporting requirements detailed in Ordering Paragraph 21 of Decision (D.) 14-03-029.

a. Background on CES-21

The CES-21 program is a public-private collaborative research and development program between the Joint Utilities and LLNL. The projects utilize joint teams of technical experts from the utilities, LLNL, industry, academia, and other contractors as appropriate to meet the research objectives consistent with the approved CES-21 Program. For more details on the Regulatory History around the CES-21 program, please see *Appendix B - Program Regulatory History*.

b. CES-21 Program Components

Cybersecurity Project: Intended to research automated response and next-generation security capabilities that could more effectively protect critical infrastructure against cyberattacks. Due to the time criticality and increasing volume of cyberattacks, automated response capabilities and new ways of securing utility communications are an increasingly important strategic goal for ICS cybersecurity systems.

Grid Integration Project: Models future iterations of the grid to study the applicability of planning, flexibility, and reliability metrics (such as the 15% Planning Reserve Margin) under the future grid conditions caused by increased renewable energy penetration and market demand.

c. Industry Trends Impacting Program and Projects

Cybersecurity Project

2017 continued to be a prominent year for cyberattacks against industrial control systems owners and operators. This continues the trend of increasing cybersecurity threats to utilities and ICS systems:

- A 2017 report by Dragos ICS Threat Intelligence provided significant information on each aspect of the 2016 Ukraine attack: the tactics, techniques, and procedures (TTP) used by the attacker(s), the system impacts, and the resulting recovery efforts. The malware framework, coined CrashOverride, is highly sophisticated and designed to take a specific action against the targets, including hampering recovery efforts. It is designed to leverage the inherent trust in the grid system communications protocols, rather than exploiting known or unknown vulnerabilities. Though the malware were designed to target European SCADA systems, researchers are confident that CrashOverride can be adapted to the US's common SCADA protocol with little effort.
- In 2016, the Gartner group estimated that by 2020, more than half of major new business processes and systems will incorporate aspects of Internet of Things (IoT), implying a burgeoning $5 billion black market leveraging IoT assets. Cybersecurity researchers at F5 Labs assessed that IoT devices are becoming the "cyberweapon delivery system of choice" by today's botnet-building attackers, who are responsible for worldwide distributed denial of service (DDOS) attacks. For example, a DDoS attack occurred in Finland and disrupted heating systems for housing blocks during sub-zero weather. This

event is relevant to the electricity industry as utilities continue to extend ancillary services to customer-owned HVAC units.

- 2017 introduced new waves of ransomware, e.g. WannaCry, Petya and Not Petya. In 2016, cybersecurity analyst and luminaire, Dale Peterson (CEO of Digital Bond) predicted that it is not a matter of "if" but "when" ransomwares will make their way to the SCADA/ICS environment. In 2016, two Latin American countries experienced first-hand ICS/SCADA Ransomware occurrences, and in 2017, closer to home, a team of Georgia Tech cybersecurity researchers demonstrated, in a proof of concept experiment, that ransomware can be delivered onto a US-based ICS/SCADA environment.

Given these recent cyberattacks on the electric industry and the increased frequency of these attacks, it is critical the ICS industries and governmental partners continue to increase their coordination and knowledge-sharing.

Grid Integration Project

The CPUC's transition from LTPP (Long-Term Procurement Plan) to IRP provided an additional opportunity to leverage project results and established a clear timeline for project closeout.[4] This transition helped shape the 2017 project plan and schedule, along with the specific deliverables for alignment with the IRP proceeding.

Specifically, the final phase of Grid Integration analysis explored the following areas:

- Assessing and confirming that the existing 15% to 17% planning reserve margin is adequate for higher RPS penetration.
- Estimating the system's operating flexibility requirements (primarily load following requirements) with higher RPS levels for a given electric system.
- Estimating the qualifying capacity of wind, solar, and other resource types for a system.
- Assessing the capacity and economic value of battery storage resources under different system scenarios.
- Offering recommendations as to how to confirm that a given future system has sufficient capacity and operating flexibility to meet existing reliability standards.

d. Coordination

Industry Coordination

Throughout 2017, the CES-21 Program engaged industry, federal agencies, and national labs in collaboration on cybersecurity research topics. This assisted the Cybersecurity project on two fronts:

- Research differentiated to avoid potential duplication of cybersecurity R&D, but add to the emerging state of the art.

[4] In its Dec. 21, 2016 IRP ruling, the CPUC established specific timelines for the CES-21 Grid Integration project team to submit its final report, present its findings and to receive stakeholder comments.

- Knowledge sharing on machine-speed-learning-focused cybersecurity research.

To aid this effort, in 2017 the project continued to use an Independent Advisory Committee with members from Department of Energy (DOE), North American Electric Reliability Corporation (NERC), Department of Homeland Security (DHS), Electric Power Research Institute (EPRI), Lawrence Berkeley National Lab and UC Davis. Other stakeholder organizations will be added to the Committee as appropriate. The project has also evaluated over 30 different companies and their products and engaged those with leading-edge products capable of furthering the research objectives of the CES-21 program. In addition to ongoing collaboration and partnerships with national labs (LLNL and INL), the project has also been interfacing with the National Security Agency (NSA) and John Hopkins Advanced Physics Laboratory.

The Grid Integration project was an active participant in the Integrated Resource planning process, and regularly informed its Advisory Group (with representatives from CPUC, CAISO, EPRI, and other stakeholders) regarding progress on modelling and initial results.

Internal Coordination

The CES-21 partner group (Joint Utilities and LLNL) has maintained a strong working relationship and regular cadence of meetings, including:

- Weekly meetings of the Project Leads and Program Managers to discuss progress and surface program-wide challenges.
- Quarterly in-person technical meetings to share information, lessons learned, and integration challenges, as well as understanding mutual progress and resolving coordination issues.
- Quarterly Steering Committee meetings with IOU and LLNL leadership.

3. Budget (by Year, by Research Area)

Below is the combined Actual and Forecasted spend for the three IOUs across the two projects of CES-21:

	Cybersecurity						
	Actual	Actual	Actual	Actual	Forecast	Forecast	
	2014	2015	2016	2017	2018	2019	Total
Budget Forecast	-	5,080,951	9,942,322	8,331,920	6,356,498	2,458,481	32,170,172
Commitments/Encumbrances	-	4,705,937	9,264,119	7,318,159	5,164,533	1,426,044	27,878,792
In House Project Expenses	-	375,015	678,203	1,013,761	1,191,965	1,032,437	4,291,381

	Grid Integration						
	Actual	Actual	Actual	Actual	Forecast	Forecast	
	2014	2015	2016	2017	2018	2019	Total
Budget Forecast	-	523,760	412,423	251,759	-	-	1,187,942
Commitments/Encumbrances	-	514,792	392,060	225,398	-	-	1,132,250
In House Project Expenses	-	8,968	20,363	26,361	-	-	55,692

	CES 21 Program - Total						
	2014	2015	2016	2017	2018	2019	Total
Budget Forecast	-	5,604,711	10,354,745	8,583,679	6,356,498	2,458,481	33,358,115
Commitments/Encumbrances	-	5,220,729	9,656,179	7,543,557	5,164,533	1,426,044	29,011,042
In House Project Expenses	-	383,983	698,566	1,040,122	1,191,965	1,032,437	4,347,073

Definitions:

- In House Project Expenses: all project and administrative expenses not completed through vendor or partner sub-contract.
- Commitments: Both contracted purchase orders and planned commitments.

4. Project 1 – Cybersecurity Project

a. High Level Summary

The Cybersecurity project aims to further the research of advanced cybersecurity technology and tools not currently commercially available. The project is focused on developing a research package to lay the foundations for automated threat response and new ways of securing utility communications and specific platforms for the IOUs to test vulnerabilities and remediations. This advancement in cybersecurity technology could help the Joint Utilities identify and act on advanced cyber-threats to SCADA and industrial control systems before they impact California's critical infrastructure.

The project is divided into ten tasks - each is autonomous but represents a building block that may contribute to a future system or multiple technology paths. The end result of the Cybersecurity project is the advancement of research toward a threat-aware grid architecture capable of making real-time decisions to increase the grid's survivability and resiliency.

b. Project Status Report

Please see attachment "CES-21 Project Status Reports 2017" to this report, as required by Decision 14-03-029.

c. Project Details

Objective

Due to the time criticality of cyberattacks on industrial control systems, an effective way to protect the power grid is through advanced detection and automated response capabilities. Automated response is a cybersecurity goal of growing importance as attack vectors—from a growing number of bad actors—are becoming more sophisticated and frequent. With the goal of improving reliability and operational efficiencies, MMATR is expected to:

- Enrich and streamline the gathering of threat intelligence
- Reduce the mean time to discovery and recovery
- Increase grid resiliency
- Lower risk posture
- Prevent attackers from reusing attacks

The research portfolio of CES-21 drives this strategy by offering new channels for evaluation and prioritization of threats and remediation. The project will extend the research on advanced threat detection and automated response for application across all CES-21 California IOU participants, and, ideally, private sector vendors who could productize such research for the wider U.S. utility community.

Scope

Automated response is a cybersecurity goal of growing importance as attack vectors become more sophisticated and voluminous. However, there is significant and legitimate concern about taking humans

out of the loop. These concerns include operator staff not being educated in how fast a cyberthreat can reach across the grid, concerns about what effects an automated response can have on the grid, and what kind of review will be done by humans in the loop, to name a few. As such, the research project does not include as part of its scope the development of production-level systems but will provide the research foundation for vendors and utilities to explore security automation more strategically.

The scope of individual project tasks may change over the course of the project, based on task progression, identification of technological requirements, and research needs. Please refer to advice letter 2656-E/3115-E/4516-E (Section 3c) for a detailed description of project scope, and see Appendix A for details on the scope of each task within CES-21. If any of the current tasks change significantly during the research, the CES-21 Program Managers will inform CPUC Energy Division.

Deliverables

To meet the Cybersecurity project's main objective of researching next generation security capabilities to protect IOU critical infrastructure against cyberattacks, the project is researching:

- **Simulation Engine**: The Modeling and Simulation (M&S) platform's purpose is to evaluate California's transmission system's resilience against cyber threats. The M&S platform is expected to provide the following key capabilities:
    - Ability to test various MMATR technologies and concepts developed in this program at scale to evaluate performance, and to uncover any unintended, negative externalities introduced by automation.
    - Modeling and simulation of grid and network devices to safely evaluate failures in a virtual environment to determine impact of cyber threats when applied at scale.
    - Assisting in cybersecurity planning exercises to inform strategic investment and design decisions.
    - Matching of anomalous ICS behavior with most probable cyber scenario cause(s) and associated set of recommended remediation actions.
- **Physical Test Bed Package:** A physical test bed environment, including substation equipment to test for vulnerabilities and potential mitigations, is being implemented at the Idaho National Laboratory collaborating with the National SCADA Testbed and Transmission and Distribution (T&D) test configurations. The reference control system architectures built here will also be used to test various research results offered by the CES-21 Cybersecurity Project.
- **Automated Response Research Package:** The research objective of the package is to provide new understanding of the logistical challenges, ICS priorities of automated threat response, and secure automated remediation of threats in pursuit of responding at machine speed to threat to the electric grid ICS components and to accelerate commercialization by vendors. As such, the research package does not have the goal of developing production-level systems but will provide a research foundation for vendors and utilities to explore security automation and orchestration more strategically. This package will include research on:

- *Advanced Threat Detection* – The goal of advanced threat detection research is to leverage ICS data collected from devices to detect and identify sophisticated and previously unknown ICS cyberattacks. Advanced threat detection will explore various methodologies, using whitelisting machine learning and artificial intelligence, to evaluate possible resilient mitigation strategies for emerging ICS threats.
- *Indicator and Remediation Language (IRL)* – IRL is a core component of a MMATR capability and will be used to describe machine readable and actionable ICS indicators of compromise and remediation logic. STIX (Structured Threat Information eXchange) is the standardized language selected for the IRL research. CES-21 research findings have been submitted and accepted as extensions to the OASIS standards body. These extensions will improve the ability of STIX to describe ICS indicators of compromise and remediation. This year, a graphical indicator and remediation entity is under development to accelerate the STIX IRL research.
- *SCADA Ecosystem Resiliency* – Investigation and testing on physical test beds unique to each IOU is crucial to an accurate assessment of MMATR technologies and concepts developed in the program and include the development of processes for threat and exploit prioritization and a tool to simplify IRL generation. Research into machine-readable IRL will enable more resilient control system devices through early detection of illicit behavior and machine-speed remediation via preprogrammed responses to mitigate exploits before there is an impact.
- *Secure Systems Interfaces* – This effort includes research and investigation of next generation security protocols and quantum cryptography mechanisms to protect end-to-end communications between ICS devices. Technologies developed here include:
  - *Quantum Key Distribution* – Future-proof key distribution technology for immediate detection of interception of keys.
  - *Secure SCADA Protocol for the 21st Century (SSP-21)* – Cryptographic wrapper for existing legacy ICS protocols to ensure integrity of observation data and control signals.
- *ICS Data Aggregation* –Research aggregation technologies, methodologies, and mechanisms to collect and process data from multiple, disparate sources, substation data, and threat intelligence. This effort will research test cases, test equipment, and test environments, as well as evaluate the effectiveness of data collection mechanisms.

Business Case Analysis

The value proposition and potential customer benefits detailed in the updated business case submitted as part of SCE's Advice Letter 3115-E, PG&E's Advice Letter 4516-E, and SDG&E's Advice Letter 2656-E (November 14, 2014), continue to apply to the Cybersecurity project. The Joint Utilities are managing closely to the post-SB96 budget and are maintaining budget compliance requirements.

Evaluation Metrics

ID	Requirement / Deliverable	2017 Results
1	Semiannual progress update meetings held with ED or ED-named proxies	Achieved
2	Monthly progress reports delivered to CPUC	Achieved
3	Maintain project financial governance in line with compliance requirements	Achieved
4	Establish guidelines for program management, shared responsibilities, and classification of sensitive data.	Achieved
5	Development of IOU-agnostic threat scenarios	2017: Use Case repository includes: 41 Use Cases Developed, 22 Tested, 64 Scenarios Identified
6	Development of machine-readable language conventions to describe threats	Work continues toward completing an IRL use case per each item listed in the Attacks and Mitigations matrix. Completion of these use cases and subsequent IRLs will provide a guide for others on crafting STIX files for various types of attacks and mitigations applicable. Work continues on testing IRL efficacy and modification of existing IRL as needed to help measures fall within the guideline parameters as defined in this task.
7	Ability to model and simulate threat scenarios	The development for this success metric is primarily conducted at Lawrence Livermore National Lab due to their industry-leading experience in complex modeling and simulation. Two simulations completed in 2017, including evaluation of scenarios with grid-level impact, and sensitivity studies of protection relays, with hardware-in-loop.
8	Ability to test models and scenarios using physical models of equipment configurations	The development for this success metric is primarily conducted at Idaho National Lab due to their experience hosting the Critical Infrastructure Test Range. The Idaho National Laboratory (INL) has created testing dashboards to ensure repeatable clean test environments that enable retesting of Test TMA (Threat Monitor Appliance)/IRL code when updates to the substation automation configuration or the software for the TMA/IRLs are incorporated or new IRLs are generated as new cyber threats appear. This repeatable testing provides for more automated test procedures. Another benefit of the testing dashboards is to ensure that no left behind data or memory stores could potentially skew collected test information. The INL has also created a dashboard for performance metrics collected during testing. These performance metrics can be fed into modeling and simulation parameters to reflect realistic physical hardware

		behavior. Other collection of network traffic during validation of the TMA/IRL can be used to reflect the substation automation network behavior.
9	Document learnings and requirements for integration of CES-21 funded research, and ensure non-duplication of research effort	Multiple coordination meetings held with federal agency, national lab, industry, and university representatives. Made further additions and updates to the MMATR Capability Vision Diagram.

Schedule

The CES-21 Cybersecurity project launched in October 2014 (with authority to spend beginning on December 29, 2014), and is authorized to continue up to five years until October 1, 2019. Certain tasks within the project may use the full approved timeframe; others will close once project objectives have been achieved.

CES-21 Funds Spent

Please see Section B for all budget information.

Treatment of Intellectual Property

Treatment of Intellectual Property is described by the Cooperative Research and Development Agreement (CRADA), signed by the Joint IOUs and LLNL. All IP rights retained through project development work are shared equally by the participant IOUs. As the project progresses, there are two types of IP anticipated to be produced: IP that is optimized by being protected and holds direct value to the CRADA participants and the ratepayer, and IP that best creates value by being shared with the wider security community through Open Source and other non-chargeable channels. The program's methodology to differentiate these categories is whether the research's commercial value is heavily dependent on adoption, such that without widespread adoption the material would have little or no direct value to the IOUs or ratepayer.

Status Update

2017 was a year of momentum and establishing specific research products for the project; the research teams were fully engaged across all the task areas, added numerous use cases to explore and created a path forward for possible integration of component parts of the research. Quarterly technical meetings were also held to share information and work through interdependency issues in person, and the teams meet in weekly conference calls to stay aligned and coordinated.

Program Governance and Foundational Collaboration

- The published guidance documentation on data sensitivity and handling relating to the CES-21 program; and the published procedures for managing the release of CES-21 program information to the public is being used routinely.
- Submitted monthly status reports to Energy Division and biannual check-in presentations.
- Coordination and collaboration continued with government agencies including DHS, DOE, and NSA.
- Functional requirements, inputs, and outputs were identified and updated for the following components and sub-components of the MMATR Capability Vision Diagram: data aggregation, threat detection, global analysis center, modeling / simulation, and orchestration and remediation. The functional diagram and sub-diagrams served as a vision statement for MMATR capabilities and was used to assess the progress of research under CES-21 and was used to identify research paths forward beyond the CES-21 Program.

Physical Test Bed

- Ethernet switch and temperature monitor were added to the SCE test bed; Acceptance Test Procedure was updated to reflect these configuration changes and was approved.
- The SDG&E test bed, which represents a transmission type substation, was delivered and acceptance tested at INL to prove out automated response and measuring.
- The PG&E test bed design is complete and equipment is being procured. Anticipated delivery to INL for configuration, acceptance testing and IRL package testing and analysis is March 2018. Already characterized a potential hardware-based attack on this configuration for a physics-based IRL package.

Modeling Engine

In 2017, the CES-21 team completed both the third and fourth of five planned cycles of development, utilizing and enhancing the modeling and simulation engine developed in prior years. The simulation engine represents the merging of two types of modeling systems: network data systems and grid configuration power flow models. Each of these categories has well developed examples, but they are not typically combined. Each development cycle is designed to build on the functionality of the previous cycle, with the end goal of being able to model a mid-sized grid environment and the data communications which control it.

- Cycle 3 focused on a cyberattack with a grid level impact. The three IOUs and LLNL agreed to simulate an important grid impact: system separation (islanding). The team designed and modeled a hypothetical covert communication method that could be used by an adversary to create islands in the WECC system. Dynamic simulations of the grid under these islanded conditions were then executed, showing the impacts of such islands on key transmission system parameters such as system voltage and frequency. Analysis of simulation data representing the covert communications is currently being performed in support of future cyber-threat threat detection methodologies to be implemented in the Threat Monitoring Appliance.
- Cycle 4 focused on a cyberattack involving malicious adjustment of protection relay settings. A combination of simulation, high performance computing (HPC), and optimization was used to evaluate how sensitive a grid system is to manipulation of certain settings of protection relays. The simulations embody a proof-of-concept for assisting utilities with prioritization for securing cyber-physical assets such as microprocessor-based electrical protection relays. Data from larger-scale and

higher-fidelity simulations of this type may help inform an automated threat response system on particularly critical areas of the California grid to monitor and protect.

- In response to the latest findings of the 2016 cyberattack against Ukraine's electric grid, the scope of Cycle 5, which will initiate in 2018, was adjusted from scenarios against Remedial Action Scheme (RAS) systems towards a focus on modeling and simulation of the same malware and TTPs (tactics, techniques, and procedures) involved in the December 2016 Ukraine attack. This re-scoping of Cycle 5 is expected to maximize the learnings of MMATR concepts, including the integration of TMA and utilization of STIX, especially within the context of ICS-tailored malware.

Research Package on Automated Response
(for use by wider utility community and private sector vendors)

- **Component Alignment and Potential Integration:** Developed a valid set of functional requirements as well as an organizational interface and process flow diagrams as part of efforts to document the operational concept for the MMATR Ecosystem
- **Indicator & Remediation Language (IRL):** Cyberthreat indicators are already being distributed by government entities and private industry in a qualitative, human-readable format. This initiative works to create the machine-readable threat encoding that includes key ICS functionalities. The project is developing its language enhancements to the global STIX standard, first started by MITRE. The STIX working group, administered by the non-profit standards organization OASIS, is the largest technical committee for this language and includes dozens of vendors in the information security industry. Last year, the project's enhancement to add complex time-based patterning was accepted as a working specification as part of STIX 2.0, and is an example of the project's research actively moving the industry forward to reflect ICS-specific needs. Work continues toward completing a set of IRL use cases. Completion of these use cases and subsequent IRLs will provide a guide for others on crafting STIX files for various types of attacks and applicable mitigations.
- **SCADA Ecosystem Resiliency:** In 2017 the project developed a prototype Graphical User Interface (GUI) tool called GraphIRL that simplifies the complex process of IRL development. Work continued to validate recently added functionality through testing and complete back-end database development. This tool has been created to simplify the complex process of IRL development.
- **The team has also developed a Threat Attribute Scoring Model** that assists in quantifying the threat that a particular exploit or malware may pose, for use during EMV analysis. This EMV work has included development of a methodology for EMV Behavior Attribute Scoring (BAS), which will provide prioritized lists of exploits, malware & vulnerabilities and - when coupled with the Threat Attribute Scoring Model (TASM) - will identify where to focus the development of indicators and remediation actions to prevent or mitigate grid impact. Risk management principles were applied to the EMV Scoring and Threat Scoring processes to determine proper weighting and groupings of sub-categories and descriptors in an effort to develop a risk comparison and reduction model that can be used to compare and prioritize risk mitigation efforts. We will continue to prioritize EMV for creation of indicators and courses of action (COA). Lastly, test performance scripts were written to automate portions of the indicator and remediation action testing. A consistent and repeatable process was established for testing and analysis on CES-21 test beds so that IRL packages can be tested and results compared. The testing process includes a dashboard that controls testing, collects metrics data and displays the test results, which are stored in the relational database. The dashboard can then reset the system for new testing and test data collection.
- **Data Aggregation - Serial SCADA communications:** In 2017 the Data Aggregation task was refocused on digital applications versus the original concept of Serial communications.
- **Secure SCADA Protocol for the 21st Century (SSP21):** In 2017 the project completed design and developed a reference implementation for a cryptographic wrapper designed to secure point-to-

multipoint serial protocols, or to act as a security layer for new SCADA applications. The program has spent considerable focus on developing this specification with the open-source community, as sharing an overall protocol (rather than the specific cryptographic system used within the protocol) will not increase security exposure for a utility, while wide adoption will increase the value proposition for SCADA vendors to incorporate the protocol.

- **Quantum Key Distribution:** This cutting-edge research explores systems to protect against quantum-computing-enabled cryptography, which would make traditional security schemes obsolete. In 2017 the project successfully demonstrated a prototype of the entangled photon technology which might be used for ICS applications in the future. Incorporation of SSP21 with QKD was in an early research spiral toward the end of 2017.

5. Project 2 – Grid Integration: Flexibility Metrics Project

a. High Level Summary

Simulate the effects of using existing reliability and capacity metrics under various conditions and greatly increased renewable penetration.

b. Project Status Report

The Grid Integration project was officially completed in November 2017. Please see attachment "CES-21 Project Status Reports 2017" to this report, as required by Decision 14-03-029.

c. Project Details

Objective

The Grid Integration project seeks to develop new flexibility metrics and recommend (if appropriate) new or modified planning standards that explicitly consider operational flexibility.

Please refer to advice letters 2656-E/4516-E (Section 3B) for a detailed description of project objective.

Scope

The scope of the Grid Integration project is to develop a holistic framework (i.e., tools, models, and metrics) to study the flexibility needs of the California electrical system under higher Renewable Energy penetration.

Please refer to advice letter 4516-E (Section 3C) for a detailed description of project scope.

Deliverables

For the Grid Integration project, Resolution E-4677 provided the following key deliverables:

- Compile preliminary results and recommendations, present in a public workshop using input assumptions from the 2014 LTPP.
- Demonstrate recommended metrics/standards in 2016 LTPP using at least one of the 2016 LTPP scenarios (trajectory or expected scenario).
- Provide opportunity for 2016 LTPP parties to comment

- Provide access to a database of detailed modeling input assumptions.
- Ensure ability of LTPP parties to license and use new or improved tools (if any).
- Conduct informal training session for Commission staff on new tools and models.

Business Case Analysis

The Grid Integration project was completed and delivered according to its original business case (see "Evaluation Metrics" section below for detailed deliverables).

Evaluation Metrics

For the Grid Integration project, the requirements and deliverables specified by Resolution E-4677 helped shape the appropriate evaluation metrics. They are listed below, along with specific results delivered in 2017.

ID	Requirement / Deliverable	2017 Results[5]
1	Form a collaborative Advisory Group and meet at least once every six months to review and connect project results with relevant CPUC proceedings	Held Advisory Group calls on 3/1/2017 and 6/13/2017 to review and obtain feedback on final phase of analysis and key project findings.
2	Leverage learnings from PG&E's earlier collaborative review of planning model work	Based on the findings from the 2014 collaborative model review effort, selected the SERVM resource adequacy / production cost modeling tool to perform analysis for the project.
3	Present preliminary results and recommendations in a public workshop using input assumptions from the 2014 LTPP	Held on 1/6/2016
4	Demonstrate recommended metrics/standards in 2016 LTPP using at least one of the 2016 LTPP scenarios (Trajectory or expected scenario)	Final analysis was completed using 2016 LTPP assumptions. Project results and recommendations were presented to LTPP/IRP parties at a CPUC Integrated Resource Planning (IRP) proceeding on 8/15/2017.
5	Provide 2016 LTPP parties opportunity to comment	Following the release of the CES-21 final report, the 2016 LTPP/IRP parties were given the opportunity to provide written comments on the project's final results and recommendations.
6	Make database of detailed modeling input assumptions available	The entire set of input data used for the study, along with the final CES-21 report, was made publicly available by the Energy Division.[6]

[5] For completeness, some results delivered in earlier years are also included

[6] Located on the CPUC's website under http://cpuc.ca.gov/General.aspx?id=6442453968

7	Ensured ability of LTPP parties to license and use new or improved tools (if any)	Updated SERVM software is available for license by LTPP/IRP parties[7]
8	Offer informal training session for Commission staff on new tools and models	The Project team held several calls during the project and met with CPUC staff on 8/16/2017 to provide training and updates on the SERVM tool and the CES-21 analytical framework.

Schedule

Project was officially completed in November 2017.

CES-21 Funds Spent

Please see Section B for all budget information.

Treatment of Intellectual Property

Treatment of Intellectual Property is described by the Cooperative Research and Development Agreement (CRADA), signed by the Joint IOUs and LLNL.

Status Update

- See "Evaluation Metrics" section above for details on results delivered in 2017.

[7] www.astrape.com

6. Lessons Learned

Cybersecurity Project

- **Model Development:** In the modeling and simulation field, complete models of as-built communication networks typically do not exist. The level of model fidelity required by a simulation depends highly on the analysis that is required and will affect outcomes if not properly determined up front. Therefore, it is important for SMEs and researchers to work closely to define the problem, plan the R&D project, and analyze results.
- **Information Technology (IT) and Operational Technology (OT) Integration:** IT and OT networks, equipment, staff, and processes have historically been very separate. We are seeing the convergence of these teams beginning to happen. Most of the impetus for this convergence from the IT side is being fueled by cybersecurity concerns. Utilities are beginning this process by attempting to establish a baseline of cybersecurity software and hardware within the OT networks using traditional IT solutions. The project has shared lessons learned and research direction with OT IOU personal during quarterly technical meetings.
- **Cybersecurity Collaboration:** There is a keen interest in industry and government agencies to collaborate with CES-21 in areas of national significance for the protection of the critical infrastructure.

Grid Integration: Flexibility Metrics Project

The following are some of the high-level lessons learned during the 2017 year for the Grid Integration project:

- **System Reliability**
    - Under the assumed resource mix studied, up to 50% RPS, the CAISO system has sufficient operating flexibility to meet demand in a reliable manner, subject to the assumption that the system operator can fully access the flexibility available including curtailments and net imports
    - Sufficient load following capability must be carried in order to ensure intra-hour flexibility sufficiency – and there is a potential tradeoff between reliability and economics in calculating requirements
- **Planning Standards**
    - In terms of new planning standards, the CES-21 results suggest there is no need, at this time, to add additional flexibility-related standards for addressing reliability-related issues
    - Planning Reserve Margin (PRM) is still a useful metric to assess adequacy, but the Effective Load Carrying Capability (ELCC) of all resources needs to be accurately calculated and used in the PRM calculation
- **New Metrics** – Use of new Loss of Load Expectation (LOLE) metrics – $LOLE_{INTRA\text{-}HOUR}$ and $LOLE_{MULTI\text{-}HOUR}$ allow for greater understanding of the flexibility needs and resources. How these relate to $LOLE_{CAPACITY}$ needs to be further considered.

7. Conclusion

a. Key Results for the Year

Key Cybersecurity project results for 2017 included:

- **Indicator and Remediation Language:** Developed ICS-specific additions to industry-standard STIX language, successfully submitted for inclusion in international standard. STIX 2.0 has been officially and publicly listed as a committee specification by OASIS. STIX 2.1 has been updated to account for various use cases and extensions created during this year of IRL development. STIX 2.1 is still in development with an estimated release date in mid-2018.
- **Operator Workshop**: Successful Operator Workshop hosted at SCE in June 2017 resulting in not only informing the Operator community of CES-21, but also capturing their challenges, needs, insights and concerns. A second successful Operator Workshop was hosted at SDG&E in December 2017 that included SDG&E Operators and an Operator from SCE that participated in the first workshop, which provided continuity and facilitated collaboration.
- **Simulation Engine:** Completed the third and fourth of five planned cycles of development. Cycle 3 demonstrated the risk of system separation (islanding), while cycle 4 helped to identify the relative importance of protecting specific relays on the grid. Preliminary scoping was also conducted for cycle 5, which will focus on a Ukraine-style attack, and include the integration of TMA and utilization of STIX.
- **SSP21:** Created reference specification of Secure SCADA Protocol, and worked with open-source community to refine.
- **Quantum Key Distribution:** Built laboratory prototype of Quantum Key Distribution system for use in ICS environments. Began early research into SSP-21/QKD integration.
- **Integration:** The MMATR Capability Vision Diagram was further developed to include drill-down subcomponents for data aggregation, threat detection, a global analysis center, modeling / simulation, and orchestration and remediation.

The Grid Integration project was successfully completed in 2017. Key results included:

- **Public Workshop Presentation:** The workshop highlighted key project findings and recommendations.
- **Final project report:** Published in the IRP proceeding
- **Assumptions and Modeling Data:** The assumptions and data were made available to the public including the entire set of input assumptions and modeling data produced by the project.

b. Next Steps for CES-21 Projects

Cybersecurity Project

- **Pursue vendor engagement:** Some work streams of the project (for example, the IRL and SSP21 initiatives) are beginning to reach the stage of developmental maturity where they can be discussed with external vendors who might productize this research. The project will now begin exploring how to

partner with the vendor community to introduce the initial versions of this research and ensure that it aligns with the needs of vendors and utilities.

- **Pursue next cycle of simulation development:** The simulation will build on the components of the previous cycles to represent increasing complexity of network and grid systems, and further incorporate the virtualized deliverables of other CES-21 tasks including utilizing TMA and STIX from other project tasks.
- **Continue engaging OASIS for future STIX/TAXII and OpenC2 iterations:** Additional use cases for IRL development will be identified, described and prioritized. Continue work with the cyber threat intelligence technical committee administrated within OASIS for STIX, TAXII and OpenC2. Will continue to work with these standards groups to ensure the machine-readable languages support current and future ICS specific abilities for describing threats and remediations.
- **INL Ecosystem:** Continue IRL package and playbook testing on IOU testbeds. Initiate the development of a MMATR Requirements and Functional Specification that could be used by vendors and/or asset owners to build or purchase software, which can be used as part of a MMATR capability. Continue work to expand the development of performance metrics and instrument the test bed to collect these metrics on each device and the network. The position in the kill chain is being assessed as a metric for remediation action cost trade-offs.
- **Quantum Key Distribution:** Currently capable of generating quantum keys over dark fiber. Next steps involve research on secure delivery of quantum-generated keys over classical wireless and wireline channels.
- **Orchestration and Automation with JH-APL and NSA:** Next steps include detection of unauthorized configuration changes, and restoration of approved configuration, using security automation and orchestration. In addition, the project will seek to identify extensions to OpenC2 to describe playbooks for remediating threats to Operating Technology (OT).
- **SSP21:** Completed SSP21 specification and reference implementation using Public Key Cryptography, Quantum Keys and shared secrets. Next steps will focus on evolving the specification through open-source development with industry stakeholders, and enhancement of the reference implementation for Industrial Key Infrastructure.
- **Physical Test Bed:** The project will continue enhancing the three test beds representing the configurations of all three IOUs and joint testing and validation. The PG&E test bed will be installed at INL in March 2018. Having testbed instances of all three configurations at INL may accelerate analysis of indicators and remediation actions that are particular to each IOU. The project will also be adding components to the current configuration to facilitate testing, test data collection and monitoring of the impact during testing. These have prompted changes in the next test configuration to enable adding components, and changes to the TMA/IRL for easier validation of remediation, and indicator capture.

Grid Integration Project

Grid Integration was successfully completed in 2017.

c. Issues that May Have Major Impact on Progress in Projects

The Joint Utilities and LLNL have not identified any issues that may have a major impact on the CES-21 Program at this time.

d. Conclusion

The CES-21 Program represents a new level of collaboration between the Joint Utilities and National Labs to think expansively and quantitatively about the future technology needs of the grid. In 2017 the two projects under this program have moved from achievement of specific research objectives to completion (Grid Integration) and mature R&D project (Cybersecurity Project). The participants continue to work in close coordination and look forward to delivering even greater results over the coming year.

Appendix A – Scope by Task of CES-21 Cybersecurity Project

Task	Scope
Task 1 - Use Case Generation	Ongoing development of cyber risk scenarios with a primary focus on the transmission grid. Cyber risk scenarios will be applicable to all California IOUs and will feature use cases which are employed by individual tasks for testing. Scenarios and use cases will be developed throughout the life of the project. The project will also work on a Concept of Operations as a potential target for the Machine to Machine Automated Response end research solution.
Task 2 - Data Aggregation	Development of methods to collect Industrial Control System information (SCADA data, Substation and Network Device Configurations) and the standardization of formats for structuring CES-21 information.
Task 3 - Modeling and Simulation	Identifying and fulfilling the initial capability requirements for modeling and simulating grid and communication systems in support of other MMATR CES-21 chartered tasks. In 2016, this task completed its scope and is now closed.
Task 4 - Test Bed	Evaluating replications of IOU equipment in a physical test bed against new and cutting-edge exploits to verify responsiveness and effectiveness of MMATR solutions.
Task 5 - Advanced Threat Detection	Developing methods for monitoring and detecting anomalies in SCADA communications, processing machine readable threat intelligence (MRTI), and translating this intelligence into threat scenarios.
Task 6 - Indicator and Remediation Language	Development and maturation of a machine-readable language conventions and standards to describe ICS threats and remediation. CES-21 selected STIX (Structured Threat Information eXpression) as the standard to be used. “IRL” or Indicator and Remediation Language is the term used within CES-21 to denote the machine-readable language.
Task 7 – Software/Device Vulnerability Assessment	De-scoped in 2015
Task 8 - SCADA Ecosystem Resiliency	Developing the processes required for automatic recognition of ICS compromise and remediation in a control systems environment. Conduct operator workshops to develop and validate concept of operations; and a vendor showcase to solicit their participation.
Task 9 - Grid Stability Framework	Evaluating detection and response strategies for a wide variety of viable attack scenarios affecting the California grid, through the delivery of a modelling and simulation platform. The modeling platform will test impacts from scenarios and from MMATR solutions in ICS networks.
Task 10 - Secure System Interface Environment	Developing a SCADA Security Protocol for the 21st Century (SSP21) by providing certificate-based authentication and integrity with encryption options for any SCADA protocol. Additionally, Task 10 will include pursuing cutting edge research into secure authentication mechanisms.
Task 11 - Documentation and Integration	Provide guidelines and documentation to aid in information handling across the project, facilitating integration between tasks, and ensuring non-duplication of R&D efforts.

Appendix B – Program Regulatory History

a. CES-21 Program Regulatory Process and History

On July 18, 2011, the Joint Utilities filed Application (A.) 11-07-008, which requested authority to recover the costs for funding the CES-21 Program up to a maximum of $152.19 million over five years, with the funding shared among the Joint Utilities as follows: PG&E – 55%, SCE – 35%, and SDG&E – 10%.

In December 2012, the Commission issued D.12-12-031, which authorized the Joint Utilities to enter into a five-year research and development agreement with LLNL. This decision authorized the Joint Utilities to spend up to $30 million a year for five years on research activities, for a total of $152.19 million. The decision also allocated these costs to each of the utilities (PG&E – 55%, SCE – 35%, and SDG&E –10%) and adopted a ratemaking mechanism for each utility to permit recovery of those costs.

On September 26, 2013, Governor Brown signed Senate Bill (SB) 96, which included language that limited the scope of the CES-21 Program to cybersecurity and grid integration research and development. These projects were not to exceed $35 million over a five-year period.8 As part of SB 96, the California legislature directed the Commission to require the Joint Utilities to prepare and submit a joint report by December 1, 2013.9 In compliance with this legislative directive, the Joint Utility Report described:

1. Scope of all proposed research projects
2. How proposed projects may lead to technological advancement
3. How proposed projects may lead to potential breakthroughs in cyber security and grid integration
4. Expected timelines for concluding the projects.[10]

On March 27, 2014, the Commission approved D.14-03-029, which modified D.12-12-031 to comply with SB 96. In this decision, the Commission:

- Reduces the CES-21 budget to $35 million (including “franchise fees” and “uncollectibles”) over a five-year period
- Limits areas of research to “cybersecurity” and “grid integration”
- Reduces the governance structure to three Program Managers from PG&E, SCE and SDG&E
- Revises budget split to PG&E – 50%, SCE – 41%, and SDG&E – 9%
- Voids any CES-21 program management expenditures incurred to date and caps future administrative expenses to no more than 10% of the total CES-21 budget
- Requires enhanced Legislative and Commission oversight of the CES-21 Program
- Revises the CRADA guidelines and project criteria accordingly

[8] SB 96 added Section 740.5 to the Public Utilities Code.
[9] Public Utilities Code Section 740.5 (e)(1).
[10] Submitted to the Commission on November 27, 2013.

On April 25, 2014, the Joint Utilities filed Advice Letter 4402-E, which sought Commission authorization to implement the CES-21 Program pursuant to D.12-12-031 and D.14-03-029. The Commission approved advice letter 4402-E in Resolution 4677-E on October 2, 2014.

In compliance with Resolution 4677-E, on October 9, 2014, the Joint Utilities filed Advice Letter 4516-E with updated CES-21 business cases, an updated CRADA, a letter from LLNL confirming that the cybersecurity project reflects a new contribution and does not duplicate past research efforts, and an updated Joint Utility Report on the scope of the CES-21 Program's proposed research projects.

The Commission also approved advice letters filed by the Joint Utilities, pursuant to D.12-12-031, to create a CES-21 balancing account or modify an existing balancing account to collect money related to CES-21.

The Commission requires the Joint Utilities to submit an annual report that provides information on the operations of the project, including projects funded, the results of the research, the efforts made to involve academics and other third parties, and the intellectual property that results from the research by March 31 of each year of the program. The Commission also requires the Joint Utilities to submit a report required by Public Utilities Code Section 740.5(e)(2) summarizing the outcome of all funded projects, including an accounting of all expenditures by program managers and grant recipients on administrative and overhead costs, and whether the project resulted in any technological advancements or breakthroughs in promoting cybersecurity and grid integration.

b. Pre-Filing Workshop Results

In D.14-03-029, the Commission required the following:

> "As part of the Supplemental Advice Letter process, the Project Managers, in cooperation with Energy Division, shall hold a public workshop including the California Public Utilities Commission at least 45 days in advance of the filing to discuss the proposed research and priorities and to review the business case for proposed research. The Commission shall review the Tier 3 Supplemental Advice filing to ensure its consistency with the policy requirements adopted in this decision and enumerated in Ordering Paragraphs 15-16." (D.14-03-029, OP 18)

In 2017, the Joint Utilities did not file any Supplemental Advice Letters, and as such did not hold any public workshops.

Attachment 1

CES-21 Project Status Reports 2017

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY
2017 ANNUAL REPORT
March 31, 2018

ATTACHMENT 1
PROJECT STATUS REPORT TO ACCOMPANY ANNUAL REPORT

Column	Information Reported by the Joint Utilities	Response
A	Investment Year	2017
B	Project Name	California Energy Systems for the 21st Century
C	Project Type	Grid Integration
D	A brief description of the project	The CES-21 Flexibility Metrics and Standards project will study and recommend, if appropriate, alternative planning metrics and standards that explicitly consider operational flexibility needed to integrate increasing levels of renewable generation. The project also aims to supplement present and future Long Term Procurement Plan (LTPP) modeling studies with an alternative set of standards and an analytical framework. The CES-21 Flexibility Metrics and Standards project will utilize a joint team of technical experts from industry, software vendors, Utilities and the Lawrence Livermore National Laboratory (LLNL). The Grid Integration Project ended in 2017 and will not be reported on in future years.
E	Date of the award	October 2, 2014
F	Funding Amount	$2,000,000
G	Funds Expended to date: Contract/Grant Amount	$1,132,250
H	Funds Expended to date: In house expenditures	$55,692
I	Funds Expended to date: Total Spent to date	$1,187,942
J	Description of why this project was selected above other	Grid Integration is a State of California priority since new operating flexibility metrics are needed for long-term resource planning in California. Improvements to methodology and existing models, or new models, are also needed to reduce the cost, and/or the uncertainty about the resource adequacy of planned resources, to integrate greater amounts of intermittent renewables.
K	Administrative and overhead costs to be incurred for each project (In-house)	$200,000 estimated administrative and overhead costs
L	Intellectual Property	No intellectual property was been brought forward to date
M	Update Year	N/A
N	Update	N/A

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY

2017 ANNUAL REPORT
March 31, 2018

ATTACHMENT 1
PROJECT STATUS REPORT TO ACCOMPANY ANNUAL REPORT

Column	Information Reported by the Joint Utilities	Response
A	Investment Year	2017
B	Project Name	California Energy Systems for the 21st Century
C	Project Type	Cyber Security
D	A brief description of the project	The CES-21 MMATR project is a public-private collaborative research and development project between PG&E, SCE, SDG&E, Lawrence Livermore National Laboratory (LLNL) and other entities (industry, academia, etc.) dependent on capabilities needed to meet the research objectives . The objective of the CES-21 MMATR project is to apply computationally-based and other problem solving resources to the emerging challenges of the 21st century electric system of California. The CES-21 Program will utilize a joint team of technical experts as best fits the research objectives from the Utilities, Industry, Academia, Lawrence Livermore National Laboratory (LLNL) and other National Laboratories. The team will combine data integration with advanced modeling, simulation, and analytical tools to provide problem solving and planning necessary to achieve California's ambitious energy and environmental goals for the 21st century.
E	Date of the award	October 2, 2014
F	Funding Amount	$33,000,000
G	Funds Expended to date: Contract/Grant Amount	$21,288,215
H	Funds Expended to date: In house expenditures (Through 2017)	$2,066,978
I	Funds Expended to date: Total Spent to date	$23,355,193
J	Description of why this project was selected above other	Grid Cybersecurity is a national and State of California priority due to the risk and potential impact a cyber incident can have on the grid.
K	Administrative and overhead costs to be incurred for each project (In-house)	$3,300,000 or less estimated administrative and overhead costs
L	Intellectual Property	Possible intellectual property is under consideration based on current R&D activities.
M	Update Year	N/A
N	Update	N/A