Pacific Gas and
Electric Company™

77 Beale Street
San Francisco, CA 94105-1814

Mailing Address
Pacific Gas and Electric Company
P.O. Box 770000
San Francisco, CA 94177-0001

March 31, 2017

Timothy Sullivan
Executive Director
California Public Utilities Commission
505 Van Ness Avenue
San Francisco, CA 94102-3298

Subject: California Energy Systems for the 21st Century (CES-21) Annual Report - 2016

Dear Mr. Sullivan:

The 2016 CES-21 annual report is submitted by Pacific Gas & Electric Company (PG&E), on behalf of itself, Southern California Edison Company (SCE) and San Diego Gas and Electric Company (SDG&E), 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 third parties, and intellectual property that results from the research.

Please contact George Zahariudakis at gxz5@pge.com or 415-973-2079, Aaron Renfro at Aaron.Renfro@sce.com or 714-895-0570, or Kellen Gill at KGill@semprautilities.com or 619-696-2972 regarding any questions about this report. Thank you.

Attachment

cc: Maria Sotero, CPUC, Energy Division
David Huang, CPUC, Energy Division
George Zahariudakis, PG&E, Regulatory
Alexander Boutelle, PG&E, Program Manager
Aaron Renfro, SCE, Regulatory
Joy Weed, SCE, Program Manager
Kellen Gill, SDG&E, Regulatory
Corey McClelland, SDG&E, Program Manager

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

2016 Annual Report

March 31, 2017

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 2016 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 workstreams:

   - 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.

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

2. **Grid Integration - Flexibility Metrics Project:** As California leads the nation in Renewable Portfolio Standard (RPS) requirements, this project is working to determine if the utilities' planning assumptions and reliability metrics are applicable under future conditions. This requires 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 is led by PG&E, SDG&E, and LLNL.

b. Status of Program and 2016 Achievements

Cybersecurity Project

In 2016 the Cybersecurity project began achieving research milestones across its major work streams:

[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.

1. The **Simulation Engine** completed two cycles of development in 2016, and updated the research roadmap for three remaining cycles. The cycles are designed to build upon one another, creating building blocks of functionality that will underpin the further development in the next cycle. Simulation 1 focused on equipment-level actions and modeled the destruction of a transformer using malware-masked Supervisory Control and Data Acquisition (SCADA) communications. Simulation 2 quantified the impact of a Denial of Service attack sent from different locations. This simulation also featured the incorporation of a virtual machine created by the project's SCADA Ecosystem Resiliency task, and was the first example of being able to model the efficacy of another CES-21 work stream's deliverable.
2. The **Physical Test Bed**, after being initially sited in 2015, was established at Idaho National Laboratory (INL) with equipment representing a substation configuration. Two other substation instances, representing PG&E and SDG&E's IOU-specific equipment and configurations, may be collocated at the site, allowing comparison between the vulnerabilities and capabilities of different hardware configurations. The success of establishing this test bed also allows researchers to test the CES-21-created Indicator and Remediation Language (IRL – see below under *Automated Response Research Package*) on actual substation equipment, in order 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 set-up of IOU-equipment-specific will allow validation of how specific equipment is being modelled in the simulation engine.
3. The **Automated Response Research Package** continued to develop across a range of topic areas:
   - *Indicator and Remediation Language* (IRL): Developed ICS-specific extensions to the Structured Threat Information eXpression (STIX), an industry-leading indicator encoding language, and successfully submitted them for inclusion in STIX 2.0;
   - Prototyped method, process flow and scoring of *Exploits, Malware and Vulnerabilities (EMV)*;
   - Designed open-source specification and reference implementation of *Secure SCADA Protocol for the 21st Century* (SSP21);
   - Demonstrated prototype *ICS Quantum Key Distribution* system using entangled photons; and
   - Documented a potential *Integration Component Architecture* across tasks, to better identify potential synergies and dependencies between tasks.
4. **Program Governance and Foundational Collaboration:** The CES-21 project continued to performed outreach sessions with federal agencies and other key stakeholders to identify synergies and help ensure non-duplication. The project established an Independent Advisory Committee[3] to gather intelligence and feedback from representatives and subject matter experts of federal and regulatory agencies, academia, and the industry.

[3] Including representatives from the Department of Energy (DOE), the Department of Homeland Security (DHS), North American Electric Reliability Corporation (NERC), and the University of California at Davis (UC Davis).

Grid Integration – Flexibility Metrics Project

In 2016, the Grid Integration project expanded its simulations of the Western Interconnect, successfully modeling every generation unit and load zone across the region. The modeling allowed detailed examination of power flows between regions and their impact on the California grid's need for operational flexibility. The project also began extracting from the rich set of modeling results initial insights that may assist the development of flexibility guidelines for future resource planning activities.

Specific highlights from 2016 include:

- Completed modeling of the full Western Electricity Coordinating Council (WECC) representation, using the 2024 Transmission Expansion Planning Policy Committee (TEPPC) dataset, which included over 4,000 generation units and over 30 distinct electric Balancing Authorities.
- Deployed the model (with full WECC representation) on the LLNL High Performance Computing (HPC) platform, demonstrated a 1,000% gain in run-time efficiency. This level of modeling is highly computationally intensive, and benefitted from the platform the project developed to leverage the HPC environment.
- Researched and explored alternative methods to estimate Load Following requirements[4] in order to meet a system's unique renewable integration challenges.
- Explored the potential use of the Electric Power Research Institute's (EPRI) highly visual InFLEXion software as a companion tool to illustrate a given system's ability to provide operational flexibility over different time intervals using SERVM results.

The results of the Grid Integration project are aligned with the Long-Term Procurement Planning (LTPP) and the CPUC's newly-created Integrated Resource Planning (IRP) proceedings, and interfaces with the stakeholders of that proceeding through CES-21 advisory group calls and public meetings. The delays in the release of the 2016 LTPP data elements held back simulation runs on the SERVM model, final inputs from external stakeholders were received in Q4 of 2016, and the final phase of simulations and results socialization will occur in 2017.

c. Lessons Learned

Cybersecurity Project

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

- **Applicability of Orchestration:** Through collaborating with the National Security Agency (NSA) and the Johns Hopkins Applied Physics Lab (JH-APL), the project has learned the importance of orchestration tools, which coordinate the response of remediation tactics. The orchestration market is growing aggressively, but is not focused on ICS-specific system needs, and the CES-21 team is working to research and identify the areas for enhancement that will allow such platforms to provide solutions for utilities and other critical infrastructure stakeholders.

[4] Operating reserve used to balance routine load and generation variability across several market dispatch intervals, typically within an hour.

- **Model Development Cycle Time:** In the original work plan, the assumption was made that the development cycles would be increasingly shortened, as smaller use cases are pursued using the foundational work of the first simulation use cases. Due to the time-intensive process of aligning development work with subject matter expertise input from operators, the project found that the second cycle was not significantly shorter than the first (approximately six months). In the interest of ensuring the project is able to gather the maximum benefits leveraging the funding allotted, it is likely that multiple tasks such as the Simulation and SCADA Ecosystem Resiliency will extend their schedule to the full approved program length of five years.
- **Grid Operator and End User Interaction:** Early involvement and review with operators and end users has helped center research focus on appropriate tools and displays of information for operations. However, the project has also encountered concern over removing humans from operational control of cyber-defenses. This level of caution reinforces the project's focus on foundational research rather than production-ready, integrated product development.
- **Standards Bodies**: When contributing to standardized languages that are overseen by a standards body (for instance, OASIS overseeing STIX), sufficient time and resources must be allocated to the development process, as these standards bodies require rigorous substantiation and verification before implementing improvements. This dependency on external partners supports the decision to use the full approved program length for certain tasks.

Grid Integration

Initial findings presented to the public at a Commission workshop in January 2016 generally hold when modeling with a full representation of WECC. Additional learning outcomes from 2016 include:

- Various methods of estimating load follow reserves are emerging and can be evaluated based on trade-offs between cost and system reliability.
- A grid system's ability to provide operational flexibility varies over different ramping intervals throughout the day. In other words, the most challenging ramping needs may occur over a four-hour time window, but this window depends on various factors and is less predictable for planners than determining peak demand (which is typically midday on the hottest days of the year).
- Deploying a desktop based application onto an HPC platform requires dedicated trials and testing. Refinements to software are sometimes necessary to enable the application to fully utilize the thousands of cores of computing power.

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 year 2016 was one in which this collaboration moved from establishing working relationships to actually delivering research accomplishments. The Grid Integration project has nearly completed its overall objectives, and currently expects to publish its final results in 2017. The Cybersecurity project has begun to accumulate real world research deliverables, including:

- Successfully updating a global threat indicator language to support key utility functionalities;
- Developing a reference implementation for securing SCADA communications; and

- Beginning to demonstrate cross-pollination between the individual tasks (e.g., simulating in the modelling platform a piece of functionality developed by the Secure SCADA Ecosystem workstream).

The program participants are proud to begin reporting 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 2016 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 OP 21 of 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 utilizes 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

This past year has seen prominent cyberattacks against ICS owners and operators, which continues the trend of increasing cybersecurity threats to utilities and ICS systems:

- Industrial control system attacks remain frequent and persistent. The U.S. Government's *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT), which provides incident response services to critical infrastructure organizations, reported a similar number of new incident tickets as in 2015. Electric utilities continue to report numerous external attempts to scan their networks for exposure; cumulative ICS scanning attempts are in the millions.
- Many of the most serious attacks occur between nation states. Though the Sandworm attack (which used the BlackEnergy trojan to deploy KillDisk malware) against the Ukrainian power grid occurred in December 2015, the ramifications of this first large-scale successful attack against an electric grid continued to be felt throughout 2016. The Ukraine power grid was again attacked in December 2016, causing parts of the Ukrainian capital Kiev to go dark. These are some of the first well-publicized examples of cyberwarfare among sovereign states and many experts fear it is a harbinger of future methods of state warfare.
- The range of adversaries against ICS is wider than just nation states. A Turkish-based energy and gas provider's website was attacked by Anonymous, such that financial, maintenance, and personal records were stolen. Ransomware attacks by profit-minded hackers were also used against municipal and utility

actors. In May, the Lansing Board of Water & Light (BWL), a Michigan municipal utility, was the subject of a ransomware attack after an employee opened an email with an infected attachment. In November, the San Francisco Municipal Railway (MUNI) transport system was impacted by a ransomware attack which did not penetrate the fare system firewalls but forced the system to run un-ticketed service for a day. These attacks are significant because they represent the diversification of utility adversaries beyond state actors, disgruntled employees, and amateur mischief makers. The utility industry has not traditionally been seen as a profit center (as opposed to financial and retail institutions) for cyber criminals, and this attitude may be changing.

- A new trend in 2016 involves the use of IoT (Internet of Things) devices as both a target and vector of attack. For example, a distributed denial of service 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 heating, ventilation and air conditioning units.
- Also in 2016, details of the virus/malware outbreak at the Gundremingen (Germany) nuclear facility were made public. While there was no destruction of data, nor loss of control due specifically to the Conficker worm and other malware used in this attack, this is the third reported cybersecurity-related incident involving a nuclear plant (the other two were in Japan and South Korea, both in 2014).

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

Grid Integration Project

In February 2016, the CPUC issued an Order Instituting Rulemaking to establish the Senate Bill (SB) 350 IRP proceeding that subsumed the previous LTPP proceeding. The transition from LTPP to IRP was an evolving process that required months of stakeholder discussions and Commission deliberations. The transition impacted project scope and schedule, but also provided an additional opportunity to leverage project results and established a clear timeline for project closeout.[5]

In terms of scope and schedule, the project team has to develop a complete California Independent System Operator (CAISO)/WECC modeling data set (whereas in the previous LTPP proceedings, the CAISO developed and provided this data to parties). The December 2016 IRP ruling required the project team to present its findings in Q1/Q2 of 2017. As a result, the project team expanded its contract with Astrape Consulting to provide funding for the additional work and established a revised work plan extending the project into 2017.

In addition to aligning schedule with the CPUC ruling, the revised work plan highlights the Grid Integration project's specific contributions to the IRP. The Grid Integration project has aligned its project schedule and identified specific ways to contribute to the IRP:

[5] In its December 21 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.

- 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 and solar for a system; and
- 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 2016, the CES-21 Program has engaged industry, federal agencies, and national labs in collaboration on cybersecurity research topics. This has assisted the Cybersecurity project on two fronts:

- Research on potential duplication of cybersecurity R&D; and
- Knowledge sharing on machine-speed-learning-focused cybersecurity research.

To aid this effort, in 2016 the project formed an Independent Advisory Committee with members from DOE, NERC, DHS, and UC Davis. Other stakeholder organizations will be added to the Committee as appropriate. The project has also researched over 25 different companies and engaged those with leading-edge products capable of furthering the research objectives of the CES-21 program. In addition to ongoing collaboration or partnerships with national labs (LLNL, Pacific Northwest National Laboratory, and INL), the project has also been interfacing with the DOE, the NSA, and the DHS.

The Grid Integration is an active participant in the IRP process, and regularly informs its Advisory Group (with representatives from CPUC, CAISO, EPRI, and other stakeholders) regarding progress on modelling and initial results.

Internal Coordination

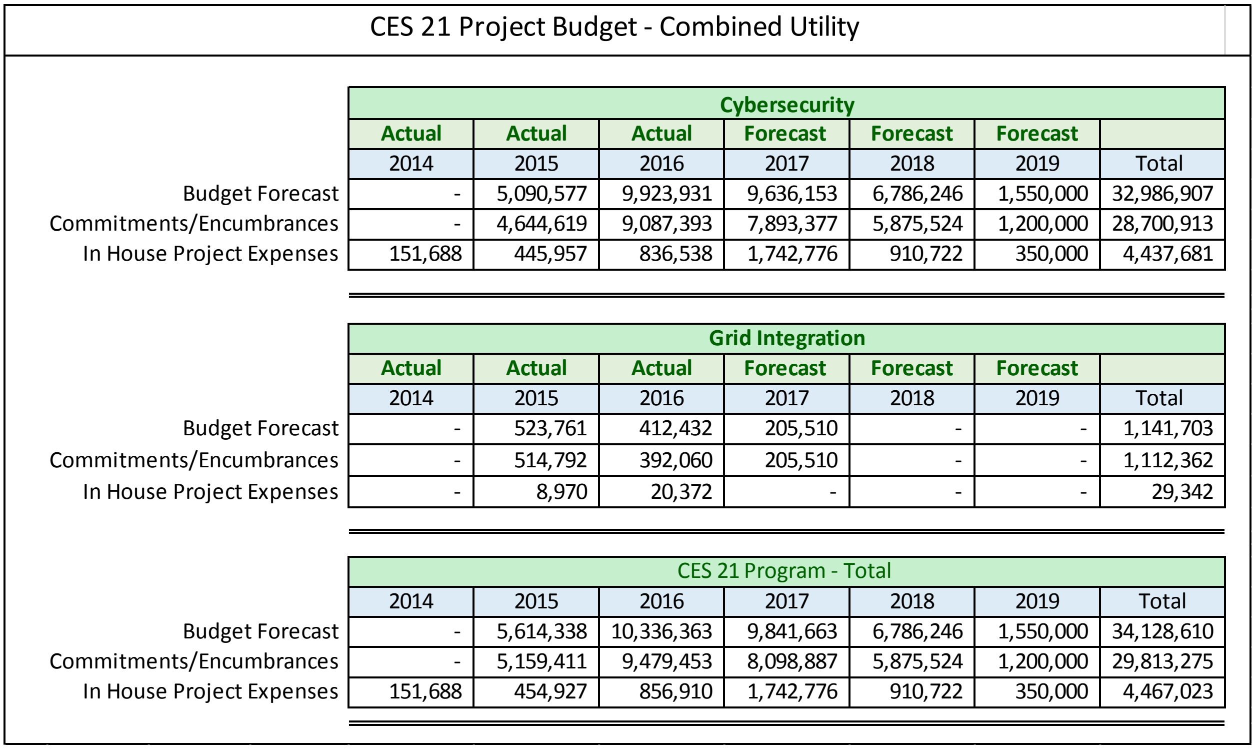
The CES-21 partner group (IOUs and LLNL) has developed a strong working relationship and regular cadence of meetings, including:

- 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; and
- Quarterly Steering Committee Meetings with IOU and LLNL leadership.

In 2016, LLNL reinforced its role in the Integration task by assigning a specific resource to coordinate questions of dependency and interaction between aligned tasks. While the tasks remain loosely coupled, there is increasingly sufficient technology output to begin seeing how components might affect each other (for example, including a virtual machine created in Task 6 as part of the Task 9 simulation). Having an ombudsman for integration issues has helped the tasks coordinate despite the significantly different subject areas.

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:



CES 21 Project Budget - Combined Utility

	Cybersecurity						
	Actual	Actual	Actual	Forecast	Forecast	Forecast	
	2014	2015	2016	2017	2018	2019	Total
Budget Forecast	-	5,090,577	9,923,931	9,636,153	6,786,246	1,550,000	32,986,907
Commitments/Encumbrances	-	4,644,619	9,087,393	7,893,377	5,875,524	1,200,000	28,700,913
In House Project Expenses	151,688	445,957	836,538	1,742,776	910,722	350,000	4,437,681

	Grid Integration						
	Actual	Actual	Actual	Forecast	Forecast	Forecast	
	2014	2015	2016	2017	2018	2019	Total
Budget Forecast	-	523,761	412,432	205,510	-	-	1,141,703
Commitments/Encumbrances	-	514,792	392,060	205,510	-	-	1,112,362
In House Project Expenses	-	8,970	20,372	-	-	-	29,342

	CES 21 Program - Total						
	2014	2015	2016	2017	2018	2019	Total
Budget Forecast	-	5,614,338	10,336,363	9,841,663	6,786,246	1,550,000	34,128,610
Commitments/Encumbrances	-	5,159,411	9,479,453	8,098,887	5,875,524	1,200,000	29,813,275
In House Project Expenses	151,688	454,927	856,910	1,742,776	910,722	350,000	4,467,023

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 cyber technology could help the Joint Utilities identify and take action on advanced cyberthreats to SCADA and ICS 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 2016" to this report, as required by D.14-03-029.

c. Project Details

Objective

The main objective of the CES-21 Cybersecurity project is to conduct research toward next generation cybersecurity techniques, including MMATR. Automated response capabilities could help utilities' critical infrastructure survive an increasing density of time-critical cyberattacks. The long-term goal is to support proactive cybersecurity problem-solving capabilities for the current and future electrical system and ultimately protect grid stability, service reliability, and public safety.

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 in taking humans out of the loop. As such, the research project does not include as part of its scope the development production-level systems, but will provide the research foundation for vendors and utilities to explore security automation more strategically.

The scope of individual Cybersecurity 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 course of 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 cyber-attacks, the project is expecting to deliver:

- A **Modeling and Simulation Platform** with associated documentation to test cyberattack scenarios under a variety of utility configurations.
  - A development roadmap for modeling and simulation capability needed to support modeling objectives and scenarios of other tasks.
- A **Physical Test Bed** which can run attack and mitigation test scenarios on actual equipment and also use IRL to exercise scenarios and better understand the responsiveness and effectiveness of MMATR solutions.
- An **Automated Response Research Packag**e to assist the industry in developing cybersecurity response technologies with ICS-specific functionalities. This package will include research on:
  - Collection of *high-impact risk scenarios* applicable to California IOUs to serve as a research foundation for other tasks;
  - An updated open-source *Indicator Remediation Language* (IRL) applicable to the Joint IOUs and encompassing their needs, and development of a web application tool to support STIX 2.0 and simplify IRL development;
  - Specification and reference implementation of *SCADA Security Protocol* encapsulating control communications to protect SCADA data integrity and support grid resilience and stability;
  - *Data aggregation* and advanced analytics capabilities to collect and analyze ICS data pertinent to defending the network and support the detection of unknown cyberthreats to ICS networks;
  - Methods and apparatus to detect and mitigate *GPS spoofing attacks*; and
  - Initial design and demonstration of prototype system to generate and distribute unbreakable cryptographic keys using entangled-photon-based *Quantum Cryptography*.
- Documentation describing a process for public release of research findings and handling of sensitive information.

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 2656-E (November 14, 2014) continue to apply to the Cybersecurity project. The Joint Utilities are managing closely to the post-SB 96 budget, and are maintaining budget compliance requirements.

Evaluation Metrics

ID	Requirement / Deliverable	2016 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

ID	Requirement / Deliverable	2016 Results
4	Establish guidelines for program management, shared responsibilities, and classification of sensitive data.	Achieved
5	Development of IOU-agnostic threat scenarios	Use case repository established, and series of initial use cases reviewed by all IOU partners.
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 continue 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 LLNL due to their industry-leading experience in complex modeling and simulation. Two simulations completed in 2016, including incorporation of Threat Monitoring Appliance (TMA) for automated threat response. Continuing to develop models and simulation with growing complexity and higher fidelity of grid behavior. Completed modeling and simulation development roadmap. Executed base capability development according to roadmap. Continued capability and scenario development under Task 9.
8	Ability to test models and scenarios using physical models of equipment configurations	The development for this success metric is primarily conducted at INL due to their experience hosting the IDAHO Critical Infrastructure Test Range. Successfully received hardware and software required for initial setup of testbed and completed initial baseline configuration. Adding components to the 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 indicators capture.
9	Document learnings and requirements for integration of CES-21 funded research, and ensure non-duplication of research effort	Multiple coordination meetings held with agency and national lab representatives.

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 from that point. 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 (IP) 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 intellectual property 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.

In March 2016, LLNL undertook a joint effort with the IOUs to obtain permission to formally release updates to GridDyn, LLNL's already-open-sourced power transmission system simulator that is used in CES-21. This effort was completed in August 2016. The program will continue to update the Commission on the status and strategy of these research release plans.

Status Update

2016 was a year of momentum for the project; the research teams were fully engaged across all the task areas and added numerous use cases to explore. 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
• Published guidance documentation on data sensitivity and handling relating to the CES-21 program; published procedures for managing the release of CES-21 program information to the public. • Submitted monthly status reports to Energy Division and biannual check-in presentations. • Coordination and collaboration continue with government agencies including DHS, DOE, and NSA. • Agreed upon expectations for defining integration potential for aligned tasks. Created initial version of MMATR capability diagram.
Physical Test Bed
• One substation instance has been successfully established, allowing the team to test the CES-21-created Indicator and Remediation Language (IRL – see below under *Automated Response Research Package*) on actual substation equipment, in order to determine if there are gaps in the current language set. Hardware components have been added to the current testbed configuration to facilitate testing, test data collection and monitoring of the impact during testing. • The project has found that staging of operational testbed components at IOU facilities - prior to shipping to INL - facilitates and expedites configuration and acceptance testing in preparation for IRL testing. • PG&E and SDG&E collected initial equipment lists and down-selected those relevant to the anticipated substation equipment. This follows similar work done by SCE in 2015.

Modeling Engine

In 2016, the Simulation engine completed two of its five planned cycles of development. 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 developmental cycle is designed to build on the functionality of the previous cycle, with the end goal of being able to model a mi-sized grid environment and the data communications which control it.

- Cycle 1 was designed to test the fundamental ability to model equipment states and the data going in and out of it. The team modeled a set of transformers and its control signals from a Human Machine Interface (HMI). Then the model was able to show how an attacker (assuming fun control of the system) could send a set of innocuous responses to the HMI while actually cycling the transformers to wear their useable life down to zero, destroying them. This represented both the first attempt to model both power and network equipment, and showed how a cyber-attack could be used to destroy actual physical equipment.
- Cycle 2 was focused on expanding to multiple virtual locations, and modeled a Denial of Service attack sent between various substations. Two attackers were modeled sending malformed packets which require a hard reboot of Remote Terminal Units (RTU). The model showed how different cadences of attacks led to different impact on affected RTUs. Additionally, the team was able to incorporate an early, virtualized version of a Threat Monitoring Appliance created by other tasks in CES-21, and modeled how it might respond to such an attack. This cycle represented a widening geographical breadth of modeling, and the first attempt at including work from other tasks into the modeling and simulation platform.

The project also completed Task 3, having met its deliverables: development roadmap and initial modeling capability development. In the course of this work Task 9 emerged as the sole user of simulation capability. Future simulation development work in support of Task 9 has been folded in to that task.

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 and 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 a global standard, first started by MITRE, called STIX (Structured Threat Information eXpression). 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. The project's enhancement to add complex time-based patterning has now been 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.
- **SCADA Ecosystem Resiliency:** In 2016 the project developed a prototype Graphical User Interface (GUI) tool that simplifies 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, which will provide prioritized lists of exploits, malware and vulnerabilities and—when coupled with the Threat Attribute Scoring Model—will identify where to focus the development of indicators and remediation actions to prevent or mitigate grid impact.
- **Data Aggregation - Serial SCADA communications:** Serial SCADA Communications use classical copper telephone services commonly used for voice communications. Legacy telecommunications equipment is being replaced by modern packet communications equipment, and so telecommunications vendors are less willing to make enhancements for monitoring and deciphering data telecommunications. As such, the Data Aggregation task is refocusing away from Serial communications.
- **Secure SCADA Protocol for the 21st Century (SSP21):** In 2016, the project designed 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 is exploring the value of developing this specification through 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 2016, the project successfully developed a prototype demonstrating how this technology might be used for ICS applications.

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

Overall, the Grid Integration project has completed three of its five phases, and is currently expected to complete in 2017. Please see attachment "CES-21 Project Status Reports 2016" to this report, as required by D.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); and
- Conduct informal training session for Commission staff on new tools and models.

Business Case Analysis

The Grid Integration project is moving forward according to its original business case. Much of the work in 2016 was dedicated to refining the robust modeling framework developed in 2015, demonstrating the ability to model a full representation of WECC, achieving efficiency gains using LLNL's HPC platform, and extracting results into EPRI's InFLEXion tool and developing useful planning guidelines.

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 2016 (additional details are provided further below in Section IX, Status Update)

ID	Requirement / Deliverable	2016 Results
1	Form a collaborative Advisory Group and meet at least once every six months to review and connect project results with relevant CPUC proceedings	Provided semi-annual updates to Advisory Group team; held number of calls with individual advisory group members to provide updates and receive feedback
2	Present preliminary results and recommendations in a public workshop using input assumptions from the 2014 LTPP	Held on 1/6/2016
3	Demonstrate recommended metrics/standards in 2016 LTPP using at least one of the 2016 LTPP scenarios (Trajectory or expected scenario)	To be completed in 2017 in the SB 350 IRP proceeding
4	Provide 2016 LTPP parties opportunity to comment	To be completed in 2017; informal comments already received following the January 2016 public workshop
5	Make database of detailed modeling input assumptions available	To be completed in 2017; provided advisory group members modeling changes to date
6	Ensured ability of LTPP parties to license and use new or improved tools (if any)	Updated SERVM software is available for license by LTPP parties
7	Offer informal training session for Commission staff on new tools and models	To be completed in 2017; project team has held number of calls and met with CPUC staff to provide updates and changes made to the SERVM tool

Schedule

In 2016, the project team extended the end date from December 2016 to June 2017 because detailed modeling assumptions to represent California and rest of WECC loads and resources from the 2016 LTPP scenarios were not available on time, or had to be independently developed by the project team, or both. The extension also allows the project to accommodate schedule changes in the 2016 LTPP proceeding and to better align the Grid Integration project with the newly introduced SB 350 IRP proceeding. The project team currently expects to present findings from its final round of analysis at an IRP workshop in Q2 of 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 CRADA, signed by the Joint IOUs and LLNL.

Status Update

Grid Integration has completed three of its five phases and is on target to complete all of its required deliverables in 2017. Key tasks completed in 2016 include:

- Presented initial analytical results at a CPUC workshop;
- Successfully completed modeling of the full WECC representation in the model (using the 2024 TEPPC dataset, which included over 4,000 generation units and over 30 distinct electric Balancing Authorities);
- Successfully deployed the model (with full WECC representation) model on the LLNL HPC platform, demonstrated a 1,000% gain in efficiency;
- Incorporated additional refinements into the model such that the planned analysis for the final phase of this project is aligned with the September 2016 CPUC ruling on modeling standards;
- Initiated research on emerging methods to estimate Load Following requirements;
- Exploring an alternative method to estimate Load Following requirement in order to meet a system's unique renewable integration challenges;
- Explored the potential use of EPRI's highly visual InFLEXion software as a companion tool to illustrate a given system's ability to provide operational flexibility over different time intervals; and
- Started work on the final analytical phase to study cases of extreme high level of renewable penetration using the latest CAISO and WECC datasets.

6. Conclusion

a. Key Results for the Year

Key Cybersecurity project results for 2016 included:

- **Indicator and Remediation Language:** Developed ICS-specific additions to industry-standard STIX language, successfully submitted for inclusion in international standard.
- **Simulation Engine:** Completed two cycles of development, including demonstration of physical damage to equipment from cyberattack and modelling of multi-substation attack scenarios.
- **SSP21:** Created reference specification of Secure SCADA Protocol, and prepared to work with open-source community to refine.
- **Quantum Key Distribution:** Built laboratory prototype of QKD system for use in ICS environments.
- **Integration:** Defined integration in the context of CES-21, obtained buy in from all four CRADA partners and designed MMATR Capability Vision diagram.

The Grid Integration project has completed three of five phases and released initial simulation results, in preparation to complete the final simulation runs and close the project in 2017. Key results include:

- **Completed modeling of the full WECC representation** (using the 2024 TEPPC dataset, which included over 4,000 generation units and over 30 distinct electric Balancing Authorities)
- **Deployed the model on the LLNL HPC platform**, demonstrating a 1,000% gain in run-time efficiency.

b. Next Steps for CES-21 Projects

Cybersecurity Project

- **Pursue vendor engagement:** Some workstreams 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.
- **Pursue next two cycles 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.
- **Continue engaging OASIS for future STIX/TAXII iterations:** In early 2017, the ballot to approve STIX 2.0 as a Committee Specification Draft goes to vote. This new STIX 2.0 version contains additions to the ICS patterning language which is a direct result of CES-21 research.
- **INL Ecosystem:** The functionality of the GUI tool discussed under SCADA Ecosystem Resiliency will be expanded. Completion of a verification and validation process will allow INL to submit this tool to the Joint Utilities for testing and evaluation. With STIX-2 moving to a data interchange format (Java Script Object Notation or "JSON"), it enables greater tool development in support of producing IRL. A training module will be completed and training will be conducted at INL to expand the number of resources that can generate IRL, which will enable a greater number of test and analysis cycles on the testbeds. Operator workshops are planned in 2017 along with a vendor showcase, which will provide valuable

feedback that will be incorporated into the development of a MMATR Requirements & Functional Specification in 2018, which will assist utilities and vendors interested in exploring greater security automation.

- **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 with JH-APL:** 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.
- **SSP21:** Currently completing Proof of Protocol and initial SSP21 specification. 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 the work to create a test bed representing the configurations of all three IOUs and joint testing and validation. 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 will produce the final required deliverables (see Evaluation Metrics in section 5C below for details) consistent with the timelines established in the December 2016 CPUC IRP ruling). These include:

- Complete final round of analysis using 2016 LTPP assumptions;
- Present project findings and recommendations in CPUC workshop; and
- Develop and publish final project report.

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. Lessons Learned

Cybersecurity Project

- Automated threat response for ICS is still in a nascent phase in the energy community. Federal agencies like DHS and NSA are beginning to conduct machine-speed learning cybersecurity research, and the DOE is funding programs to pursue cybersecurity protections of the Bulk Electric System. California is at the forefront of state-based research for this necessary technological development, and the CES-21 Program is in close contact with federal research organizations to avoid duplication and increase synergies. In 2016, CES-21 collaborated with NSA and DHS on research to further the goals of CES-21.

- Model development time is not significantly shorter during the third cycle as compared to the first. Additionally, collaborating with open-source standards bodies like OASIS requires additional time to build consensus, as compared to work just between the CES-21 partners. To make the most cost-effective use of the approved budget, the Cybersecurity project will use the full five year approved timeframe for certain tasks, particularly those that relate to the Modeling/Simulation platform.
- Monitoring and capturing data transmitted using serial communications is cost prohibitive. The project will refocus its data aggregation efforts to focus on monitoring and capturing of data after serial communications has been interworked into IP packets.

Grid Integration: Flexibility Metrics Project

Lessons learned in Grid Integration came from key project activities completed in 2016:

- The project's original 2015 findings, using a simplified representation of WECC, generally hold under a detailed representation of the WECC. These findings include that the current system contains sufficient flexibility, even as renewable penetration rises.
- Various methods of estimating load follow reserves are emerging and can be evaluated based on trade-offs between cost and system reliability.
- A grid system's ability to provide operational flexibility varies over different ramping intervals.

e. 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 2016 the two projects under this program have moved from planning/staging efforts into the achievement of specific research objectives. The participants are working 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.
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, and translating this intelligence into threat scenarios.
Task 6 - Indicator and Remediation Language	Develop and mature STIX to support CES-21 use cases.
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 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 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.[6] 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.[7] 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.[8]

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

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.

[6] SB 96 added Section 740.5 to the Public Utilities Code (Pub. Util. Code).

[7] Pub. Util. Code Section 740.5 (e)(1).

[8] Submitted to the Commission on November 27, 2013.

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 Pub. Util. 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 2016, the Joint Utilities did not file any Supplemental Advice Letters, and as such did not hold any public workshops.