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 29, 2019

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

Re: California Energy Systems for the 21st Century (CES-21) Annual Report - 2018

Dear Ms. Stebbins:

The 2018 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 Lorena Ponce at Lorena.Ponce@pge.com, John Minnicucci at John.Minnicucci@sce.com, or Tim Lyons at TLyons@semprautilities.com regarding any questions about this report. Thank you.

Attachment

cc: Amy Mesrobian, CPUC Energy Division
Johnathan Lakey, CPUC Energy Division
Judith Ikle, CPUC Energy Division
Lorena Ponce, PG&E Regulatory
Dan Gilani, PG&E
John Minnicucci, SCE Regulatory
Joy Weed, SCE
Tim Lyons, SDG&E Regulatory
John Sudol, SDG&E

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

2018 Annual Report

March 29, 2019

Table of Contents

1. EXECUTIVE SUMMARY 1

A. Overview of CES-21 Program and Plan Highlights 1
B. Status of Program and 2018 Achievements 2
C. Lessons Learned 3
D. Conclusion 4

2. INTRODUCTION AND OVERVIEW 5

A. Background on CES-21 5
B. CES-21 Program Components 5
C. Industry Trends Impacting Program and Projects 5
D. Coordination 6

3. BUDGET (BY YEAR, BY RESEARCH AREA) 8

4. CYBERSECURITY PROJECT 9

A. High Level Summary 9
B. Project Status Report 9
C. Project Details 9

5. LESSONS LEARNED 17

6. CONCLUSION 18

A. Key Results for the Year 18
B. Next Steps for CES-21 Projects 18
C. Issues that May Have Major Impact on Progress in Projects 20
D. Conclusion 20

APPENDIX A – SCOPE BY TASK OF CES-21 CYBERSECURITY PROJECT 21

APPENDIX B – PROGRAM REGULATORY HISTORY 22

A. CES-21 Program Regulatory Process and History 22
B. Pre-Filing Workshop Results 23

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 (R&D) 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 2018 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 advanced remediation methods 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 advanced remediation methods 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 and Remediation Language (IRL) research has produced standardization of an indicator encoding language that has been adopted by the European Union. In addition, the secure Supervisory Control and Data Acquisition (SCADA) protocol and Quantum Key Distribution (QKD) research has produced unique capabilities demonstrated for the first time with CES-21.

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

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

[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 (IOU) or "Joint Utilities".
[2] Per the reporting requirements detailed in CPUC Decision (D.) 14-03-029, Ordering Paragraph (OP) 21.

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, and concluded in 2017. While no new standards were found to be needed, the framework developed and methods employed in this project can be leveraged to help to inform future planning activities.

b. Status of Program and 2018 Achievements

Cybersecurity Project

In 2018, the Cybersecurity project achieved significant milestones across its major work streams:

1. **Simulation Engine:** In 2018, the CES-21 team successfully completed the fifth and final planned simulation development cycle, building upon the modeling and simulation engine developed through the four previous cycles. Cycle 5 focused on the modeling and simulation of the malware and tactics, techniques, and procedures (TTP) involved in the December 2016 Ukrainian power system attack, also known as CRASHOVERRIDE or Industroyer. The team studied available literature on the attack and developed new models to support a simulation of this attack in the context of the California electric grid. The grid impacts of three scenarios were evaluated, and results suggest that such an attack could lead to voltage deviations that would likely invoke system protection. The team also analyzed communication traffic resulting from the simulation and advised the IOUs' cybersecurity teams on potentially useful Indicators of Compromise (IOC) for this type of attack.
2. **Physical Test Bed:** In 2018, four racks of PG&E equipment providing a representation of a PG&E substation were installed at Idaho National Laboratory's (INL) Physical Test Bed, which complimented the SCE and SDG&E equipment that had previously been installed at INL in 2017. Existing IRL packages were migrated to the PG&E test bed, and IRL testing began in July 2018. Having the IOUs' equipment located at INL allows for comparison between the vulnerabilities and capabilities of different hardware and software configurations. Because each of the three IOUs implements substation devices and cybersecurity controls differently from one 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. Initial planning was also conducted for an Energy Management System (EMS) that will be delivered in 2019, and connected to all three IOU test beds through the centralized System Information and Event Management (SIEM) interface.
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.
    b. *Advanced Threat Detection*: Continued to expand the number of use cases, which demonstrated the ability to detect additional real-time simulated attacks and report the activity. Added the ability to suggest and implement a Course of Action (COA) for several use cases using the Threat Monitoring Appliance (TMA).

c. *Exploits, Malware and Vulnerabilities (EMV):* Developed a process for quantifying risks and creating the accompanying risk assignments, and developed initial releases of an accompanying graphical EMV interface.

d. *ICS Quantum Key Distribution (QKD)*: Successfully demonstrated QKD in a controlled, non-production, point to point environment, and continued to reduce the footprint of the physical device to the point where it is now sized appropriately for installation in substation racks.

e. *Secure SCADA Protocol for the 21st Century (SSP21)*: Submitted SSP21 for standards body review. SSP-21 has also been integrated in the QKD technology to create a secure protocol with integrated key distribution.

f. *Integration Component Architecture*: Updated functional requirements, inputs, and outputs 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 serve as a vision statement for MMATR capabilities and have been used to assess the progress of research under CES-21 and to help assess paths forward beyond the CES-21 Program.

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. Senior officials from the Department of Energy (DOE), the Department of Homeland Security (DHS), and the state of California were briefed on grid security and CES-21 outcomes. The first face-to-face meeting with the Independent Advisory Committee[3] was also conducted at LLNL in March 2018, 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. There was no activity on this project in 2018.

c. Lessons Learned

As development across the Cybersecurity project's task areas was in full swing during 2018, the CES-21 partners identified the following areas as key to continued success:

- Feedback from IOU Security Operations Center (SOC) practitioners has provided invaluable "boots on the ground" input on the usability of the processes and tools being developed and helped partners to focus on deliverables that would be of direct benefit to IOUs when the results of these research efforts make it to production environments. This feedback has included input on the practical application of information provided to the user, the general usability of tools, and the range of automated response that is acceptable from a risk perspective.

[3] Including representatives from the DOE, DHS, NERC, and the University of California at Davis (UC Davis).

- It was also identified that automated response would require a broader definition than initially expected and would include non-action based (information only) responses. It also became apparent that the risk created by the automated response itself must be included as part of the automated response information, and would likely affect the decision chain at the IOU level.
- Externally, there has been a continued high level of interest in CES-21 from industry sectors, as well as government agencies including DOE, DHS, and the state of California. Key lessons learned from CES-21 research have been presented at conferences such as S4x18 and DistribuTECH 2018, where the exchange of research has helped to strengthen MMATR research.

d. Conclusion

The CES-21 program represents an example of successful collaboration among the CES-21 Joint Utilities, National Labs and vendors with unique experience. 2018 was a year in which this collaboration helped to create and deliver multiple research accomplishments which will help inform the future of the grid.

Previous years' modeling and simulation efforts culminated in Cycle 5, which explored the potential impacts to California's grid, as well as means of detecting and describing the malware and tactics employed in the December 2016 Ukrainian power system attack. With the installation of PG&E equipment at INL, all three IOUs now have substation instances at the Physical Test Bed. Significant progress was also made across the various sub-components of the Automated Response Research Package, including the continued development of IRL use cases and continued enhancement of EMV vulnerability scoring capabilities.

Engagement with the external stakeholder community continued throughout 2018, and the team also coordinated with and received invaluable feedback from the IOUs' SOC representatives.

As the CES-21 program enters its final year and technical work across the Cybersecurity project's task areas ramps down, an increased focus will be placed on further defining the full MMATR roadmap and identifying capabilities on that roadmap that will not have been addressed by CES-21. Emphasis will also be placed on further engaging with the vendor community, to encourage their adoption of the capabilities developed through CES-21, for the benefit of the broader utility cybersecurity community.

2. Introduction and Overview

The purpose of this annual report is to provide the Commission with a summary of the 2018 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 R&D 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: Modeled 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. The Grid Integration project concluded in 2017.

c. Industry Trends Impacting Program and Projects

In 2018, cyberattacks on ICS and Operational Technology (OT) systems continued to be prominent in the news. Specific, high-profile, targeted attacks were not as numerous, but vulnerabilities in ICS increased.[4] Common attacks on computers running Microsoft Windows, for example, can affect ICS infrastructure just as much or more than IT infrastructure. ICS infrastructure continued to see attacks related to ransomware and cryptocurrency mining as well.

- The TRITON malware was reported in late 2017 but did not make the 2017 CES-21 annual report. TRITON (also known as TRISIS) was specifically written to attack an industrial safety system rather than an ICS. The system specifically targeted was the Schneider Electric Triconex Safety Instrumented System, designed to protect equipment, people, and infrastructure from unintended consequences. This malware uniquely targeted this Safety Instrumented System, and was only discovered because of a programming error that caused an inadvertent (though safe) shutdown of the industrial process. Deeper evaluation of the TRITON code showed that the version discovered contained the ability to override safety systems, but did not contain any active plan to implement an attack. This showed an adversarial technique change from real-time, destructive intent, to long-term successful persistence. Further

[4] Symantec Internet Security Threat Report, Volume 23

investigation showed this was likely created by a nation state to potentially secure a future tactical advantage. It is evident from the systems involved and sophistication of the approach that adversaries focused on control systems have both the system knowledge and funding required to remain undetected in environments without alerting to their presence.

- ICS and OT security are increasingly becoming important topics as the number of companies addressing this cybersecurity area has increased dramatically. Both startup companies and existing security companies are entering the ICS/OT cybersecurity space.
- In February of 2018, United States (U.S.) DOE Secretary Rick Perry established a new Office of Cybersecurity, Energy Security, and Emergency Response. Many pieces of this office previously existed elsewhere in DOE, but were consolidated at the Assistant Secretary level to reinforce the importance of cybersecurity and resiliency for energy infrastructure.
- The complexity and intensity of cyberattacks in the ICS/OT space continued to ramp up with increasing public news about nation state attacks. The U.S. DHS and Federal Bureau of Investigation issued joint Alert TA18-074A through DHS's US-CERT organization in March 2018. This alert details TTP utilized by Russian state actors to conduct cyberattacks against critical infrastructure dating back at least to March 2016. Multiple popular media outlets picked up on this story and made state-sponsored cyberattacks on critical infrastructure a common topic of discussion.

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

d. Coordination

Industry Coordination

Throughout 2018, 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 differentiation to avoid potential duplication of cybersecurity R&D, but add to the emerging state of the art
- Knowledge sharing on machine-speed-learning-focused cybersecurity research

To aid this effort, on March 14, 2018 the project conducted its first face-to-face meeting between the CES-21 team and its Advisory Committee, which is comprised of members from DOE, North American Electric Reliability Corporation (NERC), DHS, Electric Power Research Institute, Lawrence Berkeley National Lab and UC Davis.

The project team also participated in several other outreach venues in 2018. Of particular note, INL hosted the Energy Sector Coordination Council in June 2018, where over 80 energy sector industry executives were briefed on CES-21 as a lead example of progress in electric utility cybersecurity. INL also shared CES-21 activities at Grid V, a classified briefing supported by NERC and the Energy Information Sharing and Analysis Center. LLNL also hosted California Governor Jerry Brown in February 2018, who participated in a briefing on the CES-21 project.

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.
- 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:

	MMATR						
	Actual	Actual	Actual	Actual	Actual	Forecast	
	2014	2015	2016	2017	2018	2019	Total
Budget Forecast	-	5,080,951	9,942,322	8,331,920	6,129,955	2,458,481	31,943,629
Commitments/Encumbrances	-	4,705,937	9,264,119	7,318,159	5,390,925	1,426,044	28,105,184
In House Project Expenses	-	375,015	678,203	1,013,761	739,030	1,032,437	3,838,446

	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	6,129,955	2,458,481	33,131,572
Commitments/Encumbrances	-	5,220,729	9,656,179	7,543,557	5,390,925	1,426,044	29,237,434
In House Project Expenses	-	383,983	698,566	1,040,122	739,030	1,032,437	3,894,138

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. 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 apply advanced remediation methods. This advancement in cybersecurity technology could help the Joint Utilities identify and act on advanced cyber-threats to SCADA and ICS before they impact California's critical infrastructure.

The project is divided into ten tasks - each 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 2018" to this report, as required by D.14-03-029.

c. Project Details

Objective

Due to the time criticality of cyberattacks on ICS, 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, prevention, and recovery
- Increase grid resiliency
- Lower risk and increase security 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 cyber threat 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.

Please refer to Advice Letter (AL) 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 advanced mitigations, is being implemented at the INL 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 advanced 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 IOC and remediation logic. STIX 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 IOC and remediation.
- *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 pre-programmed 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 cryptographic 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 AL 3115-E, PG&E's AL 4516-E, and SDG&E's AL 2656-E (November 14, 2014), continue to apply to the Cybersecurity project. The Joint Utilities are managing closely to the post-Senate Bill (SB) 96 budget and are maintaining budget compliance requirements.

Evaluation Metrics

ID	Requirement / Deliverable	2018 Results
1	Semi-annual 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	2018: Use Case repository includes 86 Use Cases Developed, 34 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 advanced mitigations. 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 LLNL, due to their industry-leading experience in complex modeling and simulation. In 2018, the fifth and final simulation cycle, which simulated a Ukraine-style cyberattack, was completed.
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 Critical Infrastructure Test Range. In 2018, four racks of PG&E equipment providing a representation of a PG&E substation were installed at INL's Physical Test Bed, which complimented the SCE and SDG&E equipment that had previously been installed at INL in 2017. Existing IRL packages were migrated to the PG&E test bed, and IRL testing began in July 2018.
9	Document learnings and requirements for integration of CES-21 funded research, and ensure non-duplication of research effort	Continued to coordinate with federal agencies, national labs, industry, and university representatives. This coordination included the first face-to-face meeting between the CES-21 team and its Advisory Committee at LLNL on March 14, 2018. Made further additions and updates to the MMATR Capability Vision Diagram.

Schedule

The CES-21 Cybersecurity project launched on October 9, 2014 (with authority to spend beginning on December 29, 2014), and is authorized to continue up to five years until October 8, 2019. The program's final report is to be filed by December 8, 2019.

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.

On January 17, 2018, the joint utilities filed AL 3175-E / 3726-E / 5215-E (Joint AL) requesting the release of the four cybersecurity R&D applications to the open source community. These applications included IRL, GraphIRL (now renamed as Structured Threat Intelligence Graph (STIG)), GridDyn and SSP-21. On September 27, 2018, the CPUC approved the open sourcing of these applications in Resolution E-4943.

Status Update

The momentum across the Cybersecurity project's task areas continued from 2017 through 2018; the research teams were fully engaged across all the task areas, added numerous use cases to explore and continued to update the 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 are 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 National Security Agency. The first face-to-face meeting between the CES-21 team and its Advisory Committee was conducted at LLNL on March 14, 2018.
- 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 serve as a vision statement for MMATR capabilities and have been used to assess the progress of research under CES-21 and to help assess research paths forward beyond the CES-21 Program.

Physical Test Bed

- The PG&E test bed was delivered to INL in March 2018, then configured and successfully acceptance-tested. A manual discovery task was performed, performance metrics scripts were generated, and vulnerability scans were completed. The performance scripts were then added into the testing dashboard through a process call instrumenting the performance scripts. Existing IRL packages were migrated to the PG&E test bed. The virtual TMA was loaded onto the testing server, which is connected to the testbed, and IRL package testing started in July.
- A CyberStrike Workshop was held at SCE for IOU Operators. The instructor module of the CyberStrike inventory was configured to enable a demonstration of an automated response capability for the participants.
- Preliminary planning was conducted to coordinate the procurement and delivery of an EMS to INL in early 2019.

Modeling Engine

In 2018, the CES-21 team successfully completed the fifth and final planned simulation development cycle, leveraging the modeling and simulation engine developed through the four previous cycles. The team also started work on two follow-on tasks: 1) prototyping a visualization system for the simulation results, and 2) implementing and evaluating an automated remediation for the fifth simulation cycle. The simulation engine represents the merging of two types of modeling systems: communication network systems and electric grid systems. 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 cycles, with the end goal of being able to model a mid-sized grid environment and the data communications that control it.

- Cycle 5 focused on the modeling and simulation of the malware and TTPs involved in the December 2016 Ukrainian power system attack, also known as CRASHOVERRIDE or Industroyer. The team studied available literature on the attack and developed new models to support a simulation of this attack in the context of the California electric grid. The grid impacts of three scenarios were evaluated. Results suggest that such an attack could lead to voltage deviations that would likely invoke system protection. The team also analyzed communication traffic

resulting from the simulation and advised the IOUs' cybersecurity teams on potentially useful IOC for this type of attack.

- Work following on from the fifth simulation cycle has started. This work involves collaboration with project partners to develop and evaluate a remediation for the simulated cyber attack of the fifth development cycle that will invoke local (non-remote control) mode on a device when an attack is detected, so as to avoid any further damage by an adversary remotely operating grid devices. The follow-on work also involves construction of a prototype visualization system for simulation results, and the crafting of an informational video outlining the modeling and simulation advances under CES-21. Work on both of these efforts has started, and the team expects to present work products and results for this follow-on work in 2019.

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

- Advanced Threat Detection – The TMA demonstrated, both through hardware and virtualization configurations, the ability to detect real-time simulated attacks, report the activity, and suggest and implement a COA. The detection is currently limited to a small set of use cases and COAs, but work continues on more complex use cases and combining multiple use cases with multiple COAs per detected event.
- Indicator and Remediation Language (IRL) – In 2018, basic IRL packages were automatically generated by the TMA based on completed IRL use cases. These packages describe, in machine readable language, the characteristics of the attack and recommended response to the pre-defined attack scenario. Once the basic premise of IRL packages proved successful, more complex IRL generation test cases were created, and continue to be tested.
- SCADA Ecosystem Resiliency – The STIG tool, previously known in the program as GraphIRL, was completed, providing researchers and users a method to visually inspect threat intelligence and see how threat information is connected. This method greatly increases an analyst's ability to comprehend threat information, and will lead to better association between IOC and reduced decision time for an appropriate COA.
- Threat Attribute Scoring Model – In 2017, the project created a separate tool for threat scoring called EMV scoring for operator-specific risk analysis. The process for quantifying the risk and creating the accompanying risk assignments was completed in 2018. Initial releases of an accompanying graphical interface for EMV give this project incredible potential for repeatable and accurate risk analysis specific to partner environments. While continued development is not planned at this time, there is interest in refining this tool or opening the tool for open source development in the future.
- 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 (QKD) – Future-proof key distribution technology for immediate detection of interception of cryptographic keys. In 2018, QKD was successfully demonstrated, and the footprint of the physical device continues to shrink and is now sized appropriately for installation in substation racks.

- Secure SCADA Protocol for the 21st Century (SSP-21) – The SSP-21 protocol was completed in 2017 and has been submitted for standards body review in 2018. SSP-21 has also been integrated in the QKD technology to create a secure protocol with integrated key distribution. The combination of these two technologies represents a response to the most basic security concerns in ICS communications.

- ICS Data Aggregation – In 2018, the competed physical test bed environments provided CES-21 partners with the ability to collect data from real world environments and will continue to support further data aggregation and data integration opportunities for the duration of the project.

5. Lessons Learned

During 2018, most of the Cybersecurity project's R&D tasks were well underway and the team benefitted greatly from the groundwork and planning completed in earlier years. With the focus primarily on delivering technology solutions, many sub-projects were advanced far enough to allow for initial demonstration of technologies and incorporation of feedback from the demonstrations into ongoing workflows for further refinement. As feedback was analyzed as part of the development cycle, the group identified lessons learned that will continue to benefit the research beyond the completion of CES-21 in 2019. The following were key lessons learned:

- Throughout 2018, there were multiple opportunities for research partners to show their initial research and applications to IOU SOC team members. This feedback provided valuable, "boots on the ground" input on the usability of the processes and tools being developed and helped partners focus on deliverables that would be of direct benefit to IOUs when the results of these research efforts make it to production environments.
- Through internal and SOC feedback, it became apparent that automated responses included a wider range of actions than initially expected and would need to include various levels of response ranging from purely informative (non-interactive) responses, to low risk or isolation responses, and finally to full counteractive automated responses. Expanding on the original automated response scope, interactions with utility groups during research led to the conclusion that in some instances, the appropriate automated response may simply be a notification to make the operator aware of a condition, rather than automating a direct action. IOUs were initially reluctant to embrace the notion of allowing automated control of their systems, and adding notifications to show the proposed system action before human authorization would help increase adoption of automated technology. In the SOC conversations, it also became apparent that there should be risk rating for automated actions to prevent situations where automated actions can be detrimental. Future modeling will be needed to assess the possible negative impacts of automated actions.
- The team noted that creating software flow diagrams during development of IRL software, which separated the software into functional subsections and drew relationships between sections, was not only helpful in being able to properly define responsibility of deliverables, but also effective at helping to keep task scope within its original definition. Further, detailing and planning tasks between partners has led to productive results both technically and in software development. In the simulation environment, the feedback cycle led to an organized and repeatable process behind the simulation design, which made execution in 2018 more efficient and productive.
- In retrospect, as partners continue to develop software and applications which can benefit the utility security community, and have the potential to be released as open source, it would be beneficial to include software code reviews specifically to address software security earlier in the development process.
- External to the CES-21 partners, standards bodies that have been integral to future usability and adoption of related technologies have proven to be a barrier to entry for anyone who is focused on expanding the standards to cover more than the original target use cases. Specifically, the review process for incorporating IRL in STIX standard extensions has been onerous and requires change applicants to be highly specialized in the standard to support ongoing integration options.

6. Conclusion

a. Key Results for the Year

In 2018, the Cybersecurity project achieved significant research milestones across its major work streams including the areas of simulation, the physical test bed, tools and applications, and community outreach.

- **Simulation Engine:** Building in complexity on previous years' simulations, Cycle 5 focused on modeling and predicting the effects of a "Ukraine-style" attack on the California T&D systems. The simulation revealed gaps and opportunities in existing data gathering processes, and added the capability to simulate automated responses from complimentary projects in CES-21.
- **Physical Labs:** In 2018, with the installation of PG&E's substation instance, all three IOUs had substation instances at INL. Having the ability to test interoperability between IOU systems and future sharing of information between the utility providers will allow real-world validation of security test scenarios, as well as further collaboration capabilities among the IOUs at a hardware level.
- **Tools and Applications**: 2018 saw the completion of tools such as STIG for graphical analysis of intelligence, threat vulnerability scoring through EMV with basic visualization capabilities, and the generation of machine-readable attack information and recommended automated responses. As the development of production-capable tools was not an expected outcome or goal of the program, the practicality and utility of the applications created within the program represent a significant achievement.
- **Security and Utility Community Contributions**: In 2018, the CPUC granted the open source release of four major program advancements, supporting and furthering the utility security community. SSP-21 offers a secure communications protocol that supports the real time needs and currently missing security of SCADA protocols. GridDyn is a simulation environment that will enable researchers to develop grid models with increasing accuracy and complexity. IRL provides ICS-specific extensions to STIX. Finally, STIG will provide security intelligence analysts a method to quickly and visually find how threats are related, and more precisely interpret threats as they appear in their infrastructure.

b. Next Steps for CES-21 Projects

The following are the key planned activities across the Cybersecurity project's work streams in 2019:

- **Vendor Engagement**: The vendor engagement work stream will result in a vendor engagement playbook that all CES-21 IOUs can leverage to drive MMATR goals. The playbook will include the priorities for vendors of CES-21 IOUs and partners, and will reflect lessons learned from a vendor engagement pilot initiative. The pilot initiative will be designed to test channels and approaches to influence STIX adoption and support of MMATR goals by the target vendor community.
- **Concept of Operations**: A Concept of Operations (ConOps) document detailing both current IOU cybersecurity processes and potential future cybersecurity processes with the adoption of MMATR will be delivered in 2019.
- **Follow-on Simulation Work**: Follow-on work involves collaboration with project partners to develop and evaluate a remediation for the simulated cyber attack of simulation Cycle 5 that will invoke local (non-

remote control) mode on a device when an attack is detected, so as to avoid any further damage by an adversary remotely operating grid devices. The follow-on work also involves construction of a prototype visualization system for simulation results, and the crafting of an informational video outlining modeling and simulation for CES-21.

- **Continued Engagement with OASIS**: The CES-21 team will continue engaging OASIS to incorporate ongoing IRL development work in future STIX/TAXII and OpenC2 iterations. A whitepaper on sample IRL development of a use case will be released, and final reporting of the IRL development task will occur. Work involving the promotion of future ICS-specific capabilities for machine-readable languages will continue through standards groups, including OASIS for STIX, TAXII, and OpenC2.
- **INL Ecosystem**: INL will continue IRL use case development and testing. IRL packages will also include statistical analysis of remediation impact to the performance of substation automation testbeds. Other planned activities include the continued development of the EMV scoring application and continued analysis of Lockheed Martin Cyber Kill Chain® and MITRE ATT&CK™ Framework for implementation into STIX as well as trade-off analysis as part of the "Expert Guided Machine to Machine Actions" portion of the five MMATR Core Concepts.
- **Open Source Release of Tools**: INL will support the open source adoption of the STIG tool. Development of the EMV Scoring tool will continue and EMV will be further evaluated as a candidate for open source release.
- **Quantum Key Distribution (QKD)**: Development work involving integration of QKD to other security tools will occur. Specifically, security events related to QKD will be integrated into threat monitoring applications and security orchestration to automate remediation actions. A paper documenting CES-21 QKD lessons learned and future RD&D recommendations will also be developed.
- **Orchestration and Automation**: Five use cases depicting Advanced Threat Detection scenarios will be documented. A whitepaper describing interoperability of security automation and orchestration will also be developed.
- **Data Aggregation**: A white paper will be created to describe the findings and recommendations for Software Defined Substation Security. A paper documenting lessons learned and future RD&D recommendations will also be created.
- **SSP21**: SSP21 work will include updates to the SSP21 specification and reference implementation documentation, demonstration of an enhanced SSP21/QKD system, and creation of a paper documenting lessons learned and future RD&D recommendations.
- **Physical Test Bed**: A modern EMS will be procured by the utilities and provided to INL in 2019. After build, configuration and acceptance testing, the EMS will be connected to all three IOU test beds via the centralized SIEM interface.
- **Integration:** The "as-is" state of the MMATR functional diagram will be completed as CES-21 tasks are closing out. The functional diagram will describe MMATR's 'as-is' state by the end of the program and identify research gaps that were not addressed in this program. Recommendations for a research path forward to achieve higher Technology Readiness Levels for MMATR will also be identified.

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 an example of successful collaboration among the CES-21 Joint Utilities, National Labs and vendors with unique experience. 2018 was a year in which this collaboration helped to create and deliver multiple research accomplishments which will help inform the future of the grid.

Previous years' modeling and simulation efforts culminated in Cycle 5, which explored the potential impacts to California's electric grid, as well as means of detecting and describing the malware and tactics employed in the December 2016 Ukrainian power system attack. Results suggest that such an attack on the California electric grid could lead to voltage deviations that would likely invoke system protection.

With the installation of PG&E equipment at INL, all three IOUs now have substation instances at the Physical Test Bed. Testing of vulnerabilities and remediations continued, and planning is underway to procure an EMS to integrate the three IOU test beds.

Significant progress was also made across the various sub-components of the Automated Response Research Package, including the continued development of IRL use cases and continued enhancement of EMV vulnerability scoring capabilities.

Engagement with the external stakeholder community continued through the first face-to-face meeting with CES-21's Independent Advisory Committee, participation and presentations at conferences, and briefings with senior officials from federal agencies and the State of California. Through coordination with the IOUs' SOC representatives, the program also obtained valuable input on the usability of the processes and tools being developed, which has helped partners focus on deliverables that would be of direct benefit to IOUs when the results of these efforts are transitioned to production environments.

As the CES-21 program enters its final year and technical work across the Cybersecurity project's task areas ramps down, an increased focus will be placed on further defining the full MMATR roadmap and identifying capabilities on that roadmap that will not have been addressed by CES-21. Emphasis will also be placed on engaging with the vendor community, to encourage their adoption of the capabilities developed through CES-21, for the benefit of the broader utility cybersecurity community.

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 develop a ConOps as a potential target for the MMATR Response end research solution.
Task 2 - Data Aggregation	Development of methods to collect ICS information (SCADA data, Substation and Network Device Configurations) and the standardization of formats for structuring CES-21 information.
Task 3 – M&S	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	Development and maturation of a machine-readable language conventions and standards to describe ICS threats and remediation. CES-21 selected STIX 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 ConOps; 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 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 R&D 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 R&D. These projects were not to exceed $35 million over a five-year period.[5] 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.[6] 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 cybersecurity and grid integration
4. Expected timelines for concluding the projects.[7]

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

[5] SB 96 added Section 740.5 to the Public Utilities Code (Pub. Util. Code).
[6] Pub. Util. Code Section 740.5 (e)(1).
[7] Submitted to the Commission on November 27, 2013.

On April 25, 2014, the Joint Utilities filed AL 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 AL 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. 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.

On January 17, 2018, the joint utilities filed AL 3175-E / 3726-E / 5215-E (Joint AL) requesting the release of the four cybersecurity R&D applications to the open source community. These applications included IRL, GraphIRL (now renamed as STIG), GridDyn and SSP-21. On September 27, 2018, the CPUC approved the open sourcing of these applications in Resolution E-4943.

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 2018, the Joint Utilities filed AL 3175-E / 3726-E / 5215-E (Joint AL) requesting the release of the four cybersecurity R&D applications, but did not file any Supplemental ALs, and as such did not hold any public workshops.

Attachment 1

CES-21 PROJECT STATUS REPORT 2018

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY
2018 ANNUAL REPORT
March 29, 2019

ATTACHMENT 1
PROJECT STATUS REPORT TO ACCOMPANY ANNUAL REPORT

Column	Information Reported by the Joint Utilities	Response
A	Investment Year	2018
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 studied alternative planning metrics and standards that explicitly consider operational flexibility needed to integrate increasing levels of renewable generation. The project also aimed 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 utilized 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 has been brought forward to date
M	Update Year	N/A
N	Update	N/A

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY
2018 ANNUAL REPORT
March 29, 2019

ATTACHMENT 1
PROJECT STATUS REPORT TO ACCOMPANY ANNUAL REPORT

Column	Information Reported by the Joint Utilities	Response
A	Investment Year	2018
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	$26,679,140
H	Funds Expended to date: In house expenditures (Through 2018)	$2,806,009
I	Funds Expended to date: Total Spent to date	$29,485,148
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