



Arnold Schwarzenegger
Governor

SECURITY RESEARCH PROGRAM: RESEARCH OPPORTUNITY ASSESSMENT

Prepared For:
California Energy Commission
Public Interest Energy Research Program

Prepared By:
Navigant Consulting Inc.



PIER FINAL PROJECT REPORT

July 2008
CEC-500-2007-045

Prepared By:

Navigant Consulting Inc.
Stanley Blazewicz
Burlington, MA 01803
Commission Contract No. 500-01-008
Commission Work Authorization No: 44-P-05

Prepared For:

Public Interest Energy Research (PIER)
California Energy Commission

David Chambers
Contract Manager

Mike Gravely
Program Area Lead
PIER Security Research Program

Mike Gravely
Office Manager
Energy Systems Research



Martha Krebs, Ph.D.
PIER Director

Thom Kelly, Ph.D.
Deputy Director
ENERGY RESEARCH & DEVELOPMENT DIVISION

Melissa Jones
Executive Director

DISCLAIMER

This report was prepared as the result of work sponsored by the California Energy Commission. It does not necessarily represent the views of the Energy Commission, its employees or the State of California. The Energy Commission, the State of California, its employees, contractors and subcontractors make no warrant, express or implied, and assume no legal liability for the information in this report; nor does any party represent that the uses of this information will not infringe upon privately owned rights. This report has not been approved or disapproved by the California Energy Commission nor has the California Energy Commission passed upon the accuracy or adequacy of the information in this report.

Preface

The California Energy Commission's Public Interest Energy Research (PIER) Program supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The PIER program, managed by the California Energy Commission (Energy Commission), conducts public interest research, development, and demonstration (RD&D) projects to benefit California.

The PIER program strives to conduct the most promising public interest energy research by partnering with RD&D entities, including individuals, businesses, utilities, and public or private research institutions.

PIER funding efforts are focused on the following RD&D program areas:

- Buildings End-Use Energy Efficiency
- Energy Innovations Small Grants
- Energy-Related Environmental Research
- Energy Systems Integration
- Environmentally Preferred Advanced Generation
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy Technologies
- Transportation

Security Research Program: Research Opportunity Assessment is the final report for the Critical Asset Assessment project (contract number 500-01-008, work authorization #44-P-05) conducted by Navigant Consulting Inc. The information from this project contributes to PIER's Security Research Program.

For more information about the PIER program, please visit the Energy Commission's website at www.energy.ca.gov/pier or contact the Energy Commission at 916-654-5164.

Please cite this report as follows:

Blazewicz, S (Navigant Consulting Inc.). 2008. *Security Research Program: Research Opportunity Assessment*. California Energy Commission, PIER Energy Systems Integration Research Program. CEC-500-2007- 045.

Table of Contents

Preface.....	i
Abstract.....	vii
Executive Summary.....	1
1.0 Introduction.....	3
1.1 Program Background	3
1.2 Assessment Objectives	3
1.3 Assessment Approach and Scope	4
2.0 Assessing R&D Opportunities	7
2.1 Framework Analysis and Baseline Interviews.....	7
2.2 Cyber Security	7
2.3 Infrastructure Hardening	8
2.4 Interdependencies and Logistics	9
3.0 Developing Priority Research Initiatives	11
3.1 Cyber Security	12
3.2 Infrastructure Hardening	13
3.3 Interdependencies and Logistics	13
3.4 Research Areas of Interest and Candidate Project Concepts.....	14
4.0 Identification of Policy Linkage and Project Scoping.....	19
4.1 Policy Linkage and Project Prioritization	19
4.2 Research Project Scoping	22
5.0 Next Steps	27
Appendices	29
Appendix A: Public Interest Screening Criteria	29
Appendix B: Research Project Scoping.....	31

List of Figures

Figure 1	Assessment Approach	5
Figure 2	Potential R&D Opportunities by Category and Topic.....	7
Figure 3	High Priority Research Areas	11
Figure 4	Stakeholder Meeting Identify Candidate Research Initiatives.....	12
Figure 5	Stakeholder Roundtable Determines Priority Research Initiatives.....	15
Figure 6	Priority Research Initiatives.....	15
Figure 7	Researcher Roundtables Identify Candidate Research Projects.....	16
Figure 8	Candidate Research Projects.....	17
Figure 9	Stakeholder Roundtable Selects Priority Research Projects.....	19
Figure 10	Prioritization Matrix Concept.....	20
Figure 11	Project Prioritization Results.....	23
Figure A-1	Legislative Guidance on Public Interest Research.....	29
Figure A-2	Public Interest Screening Criteria.....	30

Abstract

PIER Security Research Program performed a research and development (R&D) assessment to identify opportunities for the development and transfer of existing technologies and knowledge to enhance security and resiliency of California's electricity infrastructure. After the initial literature search, the program conducted series of interviews and roundtable discussions with key stakeholders and researchers active in infrastructure security. Key stakeholders in this effort are the California utilities, California Independent System Operator, and the California's Office of Homeland Security. Researchers participating in this effort include a broad range of experts from institutions as diverse as a start-up private sector technology developer to the National Labs to research centers at universities.

Through these conversations, the Security Research Program identified six priority research initiatives to strengthen California's electricity infrastructure security, and ten candidate research projects that address one of the six initiatives. After evaluating the benefits of each candidate research project to ratepayers and stakeholders, the program selected three priority research projects for implementation consideration:

1. Develop an advanced distributed sensor network optimized for utility applications.
2. Assess the feasibility of wireless technologies for enhanced data and network security below the transmission level.
3. Survey technologies to resist physical damage

Keywords: Public Interest Energy Research, PIER, Security Research Program, energy infrastructure, electric grid, emerging technologies, cyber security, infrastructure protection, resiliency, recovery.

Executive Summary

Since September 11, 2001, there has been a concerted effort in both the public and private sectors to improve the security of critical infrastructure. To address this concern as it relates to California's electricity infrastructure, the Public Interest Energy Research (PIER) Program at the Energy Commission created the Security Research Program. The Security Research Program is PIER's response to Governor's Executive Order D-67-03, which states "all state departments and agencies are directed to assist the Office of Homeland Security and the Director of the Office of Homeland Security in carrying out the purposes of this order and the functions of the Office of Homeland Security." PIER is dedicated to ensuring a robust, secure, and reliable energy infrastructure for California through its research efforts.

The Security Research Program launched a research and development (R&D) opportunity assessment to identify opportunities for the program to improve the ability of California's electricity infrastructure stakeholders to prevent, prepare for, and respond to threats, hazards, and supply disruptions. The effort began with literature search and baseline interviews with key stakeholders and select researchers. Key stakeholders in this effort were the California utilities, the California Independent System Operator, and California's Office of Homeland Security. Researchers represented a broad range of experts from institutions as diverse as a start-up private sector technology developer to the National Labs to research centers at universities. Research needs for each entity interviewed were captured, and a key stakeholder roundtable was organized to obtain consensus on California's fundamental needs in security research.

Through these conversations, the Security Research Program identified six priority research initiatives to strengthen California's electricity infrastructure security:

1. Data security for non-transmission infrastructure and emerging technologies.
2. Technologies to resist physical damage from blasts and bullets.
3. Unmanned aerial vehicles.
4. Transportation infrastructure.
5. Emerging technologies for infrastructure hardening.
6. Sensors and wireless networks for utility security applications.

Following the roundtable with key stakeholders, the program hosted a series of interviews and roundtable discussions with researchers with expertise in areas related to infrastructure security to better understand current research landscape relevant to the priority research initiatives.

Given these inputs, the program then constructed 10 candidate research projects that were critiqued and refined at the second roundtable with key stakeholders. Taking stakeholder feedbacks into account, the program evaluated each of the candidate research projects based on their value to industry and fit with PIER's objective of performing research with a high

level of public interest. Based on this evaluation, three projects emerged as the most valuable projects, in the near term, for the program to pursue:

1. Develop an advanced distributed sensor network optimized for utility applications.
2. Assess the feasibility of wireless technologies for enhanced data and network security below the transmission level.
3. Survey technologies to resist physical damage.

While much work is underway to address security vulnerabilities for the electric power infrastructure in California, technology gaps exist that could be more quickly closed with focused RD&D efforts supported by the program. The program will strive to maintain and diversify its research portfolio and to explore various implementation vehicles and partnership opportunities of to maximize the ratepayer benefits.

1.0 Introduction

1.1. Program Background

In 1996, the Legislature established the Public Interest Energy Research (PIER) Program at the Energy Commission, funding the program with payments from Investor-Owned Utility (IOU) ratepayers. Assembly Bill 1890 was enacted to ensure that the benefits obtained from important public purpose programs, such as public interest energy research and development (RD&D), would not be lost in the newly deregulated environment. Starting on January 1, 1998, California Public Utilities Code Section 381 required that California's electric investor-owned utilities (IOUs) collect at least \$62.5 million annually to fund energy-related research, development and demonstration activities.

Since September 11, 2001, there has been a concerted effort on the part of local, state, and federal government entities along with the private sector to improve the security of critical infrastructure¹. The Security Research Program is PIER's response to Governor's Executive Order D-67-03 which states "all state departments and agencies are directed to assist the Office of Homeland Security and the Director of the Office of Homeland Security in carrying out the purposes of this order and the functions of the Office of Homeland Security." PIER is dedicated to ensuring a robust, secure, and reliable energy infrastructure for California through its research efforts.

The PIER Security Research Program seeks to improve the ability of electricity infrastructure stakeholders to prevent, prepare for and respond to threats, hazards, and supply disruptions. The PIER Security Research Program aims to catalyze transfer and exploration of technologies relevant to energy infrastructure security to enhance the reliability and survivability of California's electricity grid. These technologies, when developed specifically to protect electricity-related infrastructure, could help reduce vulnerabilities that are not being adequately addressed. The program will pursue its goals in accordance with PIER's Public Interest Screening Criteria (see Appendix A).

1.2. Assessment Objectives

The electricity infrastructure stakeholder community in California has spent a significant amount of time and money addressing known security vulnerabilities in recent years. In most cases, these activities have been focused on vulnerability identification and application of available technology solutions. The purpose of this research opportunity assessment was

¹ Definition of Critical Infrastructure - "The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole." Presidential Decision Directive 63. [Online]: Available: <http://www.ciao.gov>

to identify technology areas and research initiatives that could be advanced with support from the PIER Security Research Program.

In response to these research and technology needs, PIER's Security Research Program has identified two strategic objectives:

- A statewide common operating picture (COP)² that would provide risk-based, decision-support tools to continuously manage asset integrity and perform viability monitoring to mitigate system disruptions from natural and man made disasters; and
- Statewide resilient, self-diagnosing, self-healing systems that will continue to provide service if attacked or damaged.

This research assessment effort sought to identify high priority research initiatives for PIER's Security Research Program that supports state energy policy and lays a strong foundation for the future development of the program. High priority research initiatives are those that:

- Address critical security challenges that are not being addressed by the private sector or state/federal agencies;
- Enable promising technology or create critical knowledge; and
- Support the public interest.

1.3. Assessment Approach and Scope

The research opportunity assessment was designed to quickly obtain and analyze a large body of information, and identify high priority opportunities with a high level of stakeholder involvement. The work began with a broad examination of potential vulnerabilities and related issues. This included a general literature search and interviews with experts in areas related to electric infrastructure security. This information was organized into categories and topics that could be discussed in detail during a series of in-person interviews and roundtable meetings with stakeholders and technology experts. Along the way, key issues and research initiatives were identified to ensure that limited program resources could be applied most effectively. At the end of the process, three project concepts were developed that offered high value for stakeholders and a strong fit with PIER

² Definition of Common Operating Picture (COP) – “Sensor network that is intelligent, self-monitoring, and self-healing to allow continuous operation for situation monitoring and information transfer. It would be able to feed computational models to analyze specific issues, train decision support systems, and response personnel.” The National Plan for Research and Development In Support of Critical Infrastructure Protection 2004, The Executive Office of the President, Office of Science and Technology Policy, The Department of Homeland Security Science and Technology Directorate

public interest objectives. Figure 1 illustrates the process used to identify and prioritize research initiatives and projects.

Section II of this report presents the framework of analysis developed following the initial research assessment and some highlights from the numerous interviews conducted over the course of this effort. Section III details the path to finding the high priority research initiatives and the candidate research projects. Section IV describes the process used in determining the top research project concepts resulting from this research assessment.

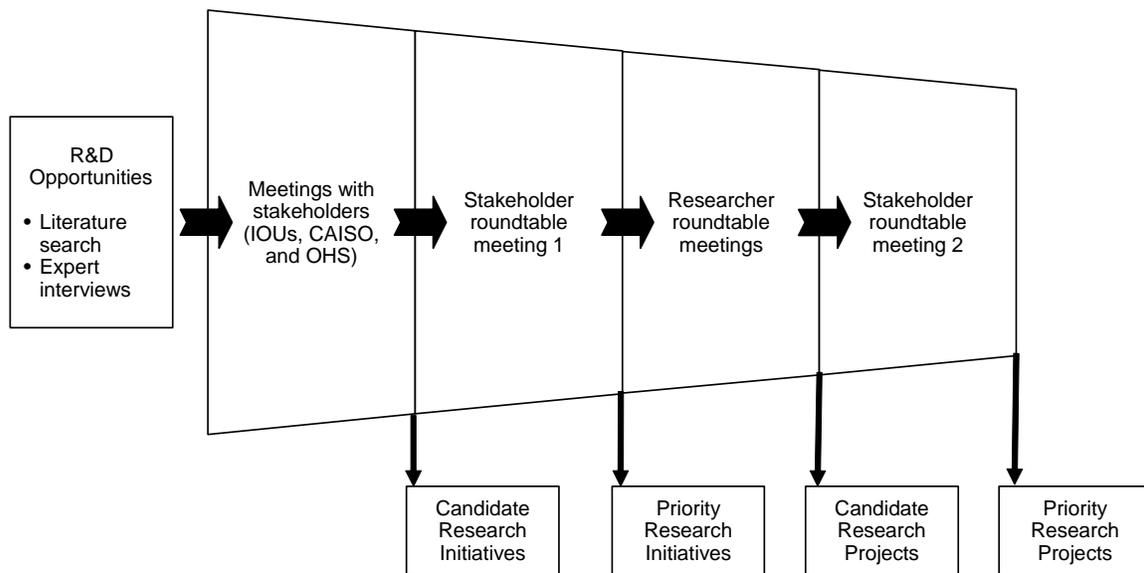


Figure 1: Assessment Approach

Source: Security Research Program: Research Opportunity Assessment

While PIER’s Security Research Program addresses the full scope of energy and related infrastructure security (e.g., electricity, natural gas, petroleum), this assessment was focused on the generation, transmission and distribution of electricity. To the extent that interdependencies between this infrastructure and other energy infrastructures yielded high priority opportunities (e.g., generation fuel supply, telecommunications, transportation, water), they were considered.

Throughout the assessment, two groups were engaged heavily: stakeholders and researchers (technology experts). The purpose of this was to ensure that the Security Research Program could quickly down-select to the opportunities with the highest potential value and best program fit. Stakeholders and researchers were initially interviewed individually in order to focus on their most pressing issues and priorities. Selected individuals from these stakeholder and research organizations were then invited to

participate in facilitated roundtable discussions where they could collectively discuss high priority opportunities identified during the interviews. Throughout the roundtable meetings, participants were directed not only to explore vulnerabilities, solutions and technology gaps, but also to specify actions that the Security Research Program could take to add significant value.

The following organizations were involved in the interviews and/or roundtable meetings:

Stakeholders

- California ISO
- California Office of Homeland Security
- Los Angeles Department of Water & Power
- Pacific Gas and Electric Company
- San Diego Gas and Electric (Sempra Energy)
- Southern California Edison

Researchers and Technology Experts

- Center for Risk and Economic Analysis of Terrorism Events (CREATE), USC
- Dust Networks
- U.S. Department of Energy (DOE)
- EnerNex
- EPRI
- Idaho National Laboratory
- KEMA
- Lawrence Livermore National Laboratory
- ManTech SMA
- DOE National Energy Technology Laboratory
- Oak Ridge National Laboratory
- Rudolph Matalucci Consultants, Inc.
- SAIC
- Sandia National Laboratory
- Technical Support Working Group (U.S. Department of Defense)
- University of California, Berkeley
- University of Southern California

2.0 Assessing R&D Opportunities

2.1. Framework Analysis and Baseline Interviews

Initial literature search results and baseline interviews with select researchers and key stakeholders led to construction of the following framework of analysis. As shown in Figure 2 below, the Security Research Program categorized R&D opportunities into three areas: Cyber Security, Infrastructure Hardening, and Interdependencies and Logistics. The program held numerous interviews with stakeholders, as well as selected researchers active in areas relevant to infrastructure security, to better understand the nature of the problems in these areas and their importance to the industry.

Cyber Security	Infrastructure Hardening	Interdependencies/Logistics
<p>Cryptography</p> <ul style="list-style-type: none"> Digital signatures Private networks <p>Configuration Management and Assurance</p> <ul style="list-style-type: none"> Policy enforcement Network management Continuity of operations tools Scanners Patch management <p>Access Control</p> <ul style="list-style-type: none"> Boundary protection (e.g., firewalls) Authentication Authorization <p>System Integrity</p> <ul style="list-style-type: none"> Antivirus management File integrity checkers <p>Audit and Monitoring</p> <ul style="list-style-type: none"> Intrusion detection systems Intrusion prevention systems Security event correlation tools Computer forensics tools <p>Proprietary Systems</p>	<p>Facility & System Design</p> <ul style="list-style-type: none"> Multi-layered defenses and buffer zones Access barriers Redundant systems (e.g., fire and life safety) Low cost retrofit structures High visibility defensive structures/systems Adaptive “islanding” <p>Sensors</p> <ul style="list-style-type: none"> Advances sensor technology Low-cost sensors Wireless sensors <p>Countermeasures</p> <ul style="list-style-type: none"> Thermal signature masks Low-cost electromagnetic shielding Advanced surveillance systems <p>Locational Considerations</p> <ul style="list-style-type: none"> Relocation of critical infrastructure (e.g., away from urban centers or underground) Decentralization of control or redundant control centers <p>Modeling and Testing</p> <ul style="list-style-type: none"> Threat analysis Infrastructure vulnerability assessment Security audit standards Scenario planning 	<p>Contingency Planning</p> <ul style="list-style-type: none"> Positioning and storage of emergency response resources System restoration-related transportation accessibility assessment Regulatory response planning to accelerate post-attack service restoration <p>Coordination</p> <ul style="list-style-type: none"> Security audit of data linkages between ISO, IOUs, munis, generators, etc. Standardization of operating rules and procedures Standardization of planning tool input and assumptions Secure emergency communication protocols <p>Fuels</p> <ul style="list-style-type: none"> Flexible fuel cost/benefit analysis Fuel supply vulnerability assessment <p>Hardware</p> <ul style="list-style-type: none"> Modular infrastructure components (e.g., transformers) Spare parts inventory control

Figure 2: Potential R&D Opportunities by Category and Topic

Source: Security Research Program: Research Opportunity Assessment

2.2. Cyber Security

2.2.1. Relevance to infrastructure and stakeholders

Information security and data management is critical to the reliability of the grid. There are concerns among the IOUs regarding enhancing SCADA/EMS security against cyber attacks. Tampering of cyber assets and control rooms could have system-wide impact to the electric grid. In addition to direct security measures against cyber threats (e.g. firewall, antivirus management), proper personnel training (e.g. policy awareness and enforcement) must be in place.

2.2.2. Stakeholder and research feedback

“PIER can’t handle sensitive information without legislative change. If it could, PIER could help the IOUs better share their information and concerns by developing an analytical process to review information. PIER can codify key security considerations in a check-list format usable by all the utilities.”

-Former Energy Commission staff

“The new NERC³ standards are pretty robust. The CEC can play an auditor role to develop scenarios to see how the utilities would respond. We haven’t set a standard beyond NERC. Developing credible scenarios is very important.”

-Utility executive

“This might be a cliché in fundamental security tenet, but you don’t want a hard, crunchy exterior and a soft, chewy interior. There must be layered security inside the perimeter. If you focus resources on enhancing perimeter security, it could lead to problems.”

-Security expert

“If you are going to wireless because of processing constraints and the amount of information they can handle, there should be a pretty robust information protection. Industry is probably going to have to address that for a wireless system to work well for them.”

-National lab researcher

“One thing we don’t have today is a computing requirement for how much computing resources need to be devoted to security. We need computer requirements, central processing unit cycles, bandwidth, and how much computer resources need to be set aside for security.”

-Security expert

2.3. Infrastructure Hardening

2.3.1. Relevance to infrastructure and stakeholders

Substations and transmission lines are critical to the electric power system. Implementing effective and cost-efficient security measures is a high priority due to the extent and sometimes remote location of the infrastructure. Three high priority opportunities were identified related to infrastructure hardening:

1. Intrusion detection and assessment capabilities
2. Resilience against physical attacks
3. Protocol for rapid recovery from the damage caused

³ North American Electric Reliability Council

If vulnerability against human threats is reduced, there is an associated benefit for natural threats such as weather, fire and earthquakes. Routine operations would also benefit from improvements in these areas, making such advancements very attractive, and much more cost effective.

The security measures must be operational in particular environment where they are installed. Given the geographical and climatic diversity across California, that implies that no one measure can be applied across all utility-owned assets. Multiple technologies must be considered and deployed for optimal protection of the assets.

2.3.2. Stakeholder and researcher feedback

“Our industry is spending a lot of money securing facilities. Reliable and cost-effective wireless CCTV and alarm systems are very desirable. It would have a significant impact in a variety of industries.”

- Utility executive

“There are three major groups of threats to the electricity infrastructure. First is natural disaster. Weather accounts for 50% of all the electrical outages and earthquakes are a major concern in California. Second is equipment failure. Terror is the third category; within the last 10 years, there were 300 terrorist attacks on electricity infrastructure worldwide. All these major events have a detrimental effect on the system. It was estimated that \$500 billion is needed to harden the entire system. Selective hardening is the most critical.”

-University researcher

“You need a consistent threat definition, since cost benefit analysis in security is extremely important. Threat spectrum needs to be identified to reduce the risk of a back door left open, as well as to not spend ourselves into the ground on security.”

-National lab researcher

“The concept of distributed sensors is nothing new in the wired world. The most critical issue is that information coming back is not spoofed. The key is to not trust one source; we need to constantly compare information against other sources.”

-National lab researcher

2.4. Interdependencies and Logistics

2.4.1. Relevance to infrastructure and stakeholders

Clear understanding of interdependencies and logistics is crucial for sustaining operational reliability of the transmission system during a time of crisis. Knowledge of fuel supplies and transportation infrastructure, and how they are connected to the grid will aid in rapid recovery from grid emergencies.

This knowledge is also necessary in bounding the threat definition. Protecting weak links within the system and prioritizing damage control and recovery processes would effectively and efficiently enhance infrastructure security.

2.4.2. Stakeholder and researcher feedback

“Natural gas is critical to electricity and drives the petroleum market. System connectivity and interdependencies would lead you to natural gas. Pipeline vulnerability is a matter of disruption in time, not just supply. Recoverability from an attack should be a major consideration. Interchangeability of equipment is important. The entire chain of events involved in recovery needs to be considered.”

-Former CEC staff counsel

“We believe that it is much more fruitful and economical if we do damage control and recovery. Interruption of service, business, and communication is the major impact of the attacks. If we can repair the damage efficiently and quickly, that may be the most valuable.”

-University researcher

“Work done in this area is in fragments. Value is in looking at transportation equipments and mapping the system to identify gaps in critical information regarding this topic to support California utilities. If you can plan ahead of time, you are already ahead of the game.”

-CAISO representative

3.0 Developing Priority Research Initiatives

Meetings with stakeholders and key researchers pointed to several high priority research areas.

High Priority Research Areas Revealed During Stakeholder Conversations		
Cyber Security	Infrastructure Hardening	Interdependencies & Logistics
<ul style="list-style-type: none"> • SCADA security enhancement • Data security best practices guidebook • Audits and red team exercises 	<ul style="list-style-type: none"> • Effective low-cost sensors • Wireless sensor networks • Cost reduction for perimeter protection 	<ul style="list-style-type: none"> • Tabletop inter-regional vulnerability assessment exercise • Natural gas pipeline vulnerability assessment • Spares inventory coordination • Transportation linkages

Figure 3: High Priority Research Areas

Source: Security Research Program: Research Opportunity Assessment

These areas were further explored to develop candidate research initiatives that could be discussed collectively at the first stakeholder roundtable meeting.

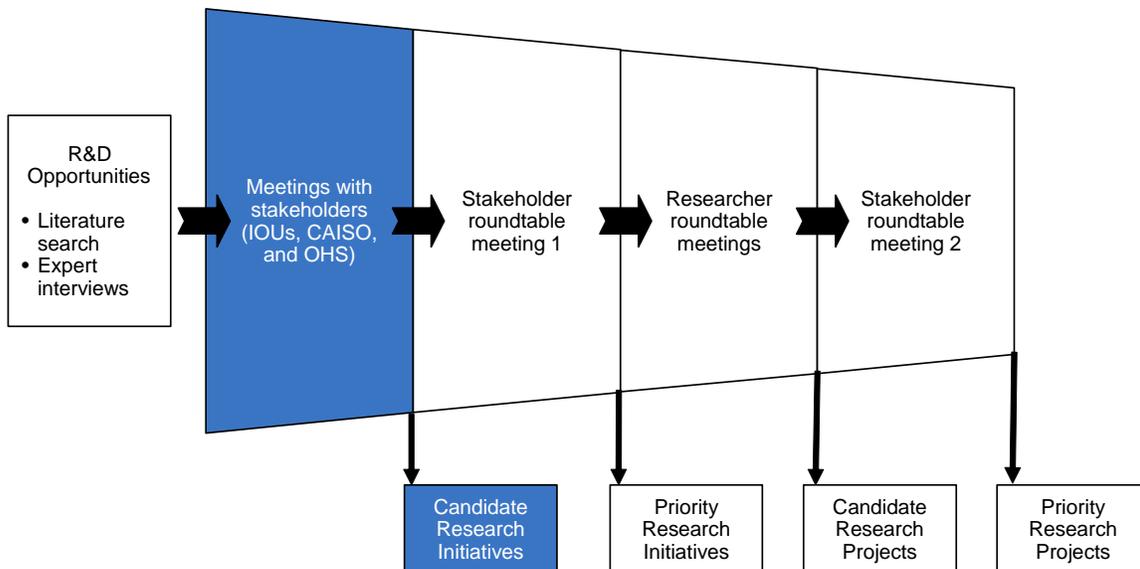


Figure 4: Stakeholder meetings identify Candidate Research Initiatives

Source: Security Research Program: Research Opportunity Assessment

3.1. Cyber Security

3.1.1. SCADA Security

Bulk power system communication and control systems such as SCADA and EMS have been identified as having potential cyber security vulnerabilities. In recent years, there has been a significant effort to address these vulnerabilities, including the NERC Critical Infrastructure Protection Committee and its Control System Security Working Group, and the establishment of the National SCADA Test Bed. While progress is being made in this area, more work could be done, particularly with regard to the communication and coordination of best practices among regional participants.

3.1.2. Red Team Exercise

The “red team” is the malicious force in a simulated conflict or intrusion. Red team exercise could be used to reveal weakness of a system and give utilities more extensive knowledge regarding security of the current grid system. It could not only uncover previously unknown vulnerabilities, but also the scale of impact from potential cyber attacks.

3.1.3. Non-SCADA Communication and Control Infrastructure

Given the increasing need for data and control technologies to manage distribution automation, advanced meter reading (AMR), phasor measurement units (PMUs) and distributed energy resources (DER), an understanding of potential security vulnerabilities is needed as current cyber security standards may not fully address the extent to which some utility systems have extended their control and data flows well beyond the transmission level.

3.2. Infrastructure Hardening

3.2.1. Perimeter Protection Enhancement

Smart CCTV (Closed Circuit Television) and 3D-VMD (Video Motion Detector) are two of the technologies currently employed in various perimeter protection systems. These technologies could be integrated to increase reliability and performance of the monitoring system by reducing false positives and negatives. In addition to implementing video-based monitoring system, unmanned aerial vehicles (UAVs) offer a promising option for perimeter patrolling. Policy randomization would create an additional factor of deterrence against malicious intruders.

3.2.2. Access Denial

Non-lethal weapons could deter intruders from tampering with the assets critical to the operational reliability of the grid. For example, some technologies include sonic stand-off systems, remote loud hailer, sticky foam and concealment/misdirection.

3.2.3. Equipment Hardening

Pumice/composite coatings could protect against physical attacks, but must not compromise the cooling systems of the equipment they are intended to protect. Using Kevlar blankets or temporary/modular armor systems could help avoid thermal problems, but they must be deployed each time additional protection is deemed necessary.

3.2.4. Advanced Sensors

One of the major problems associated with security sensors is oversensitivity processing algorithms that lead to a high number of false positives. However, this problem could be avoided by using multiple types of sensors connected to one security network. Recent technology development has significantly reduced the size of sensor nodes and the cost of the overall sensor network. The research community believes the size and cost associated with an advanced sensor network will continue to decrease over the next few years. Research on applicability and specific environmental and geographical requirements for deployment is necessary for effective utilization of advanced sensor technologies.

3.2.5. Wireless Networks

Advances in wireless technology could dramatically change the economics of security and system management applications. Current wired solutions greatly limit the application of security and control systems to only the largest and most critical facilities given the cost of implementation. However, the viability and security of wireless networks in a utility setting is not well understood.

3.3. Interdependencies and Logistics

3.3.1. Spares Inventory

Ensuring there are spares for critical components of transmission lines (e.g., HV transformers) would expedite the recovery process in cases of large-scale sabotage or malfunction. Currently, access to spares for many system components is limited and lead

times for replacement can be significant. Some spares are located in the vicinity of the in-service assets, which defeats the purpose of having the spares accessible.

3.3.2. Transportation Routing

Since high voltage transformers are too heavy to be flown, they must be transported on the ground. Securing the transportation route for the spares to be shipped is important in terms of rapid recovery from the damage incurred.

3.3.3. Vulnerability/Threat Assessment

Many of the grid vulnerabilities arise from grid interdependencies and logistics of recovery process. For the utilities to effectively protect their assets, these vulnerabilities and associated threats must be properly assessed. Doing so will allow for the utilities to properly define threat boundaries and better apply protective measures.

3.3.4. UAVs for Utility Applications

Surveying damages incurred to electric grid in case of emergency could be a challenging task; many key physical assets are remotely located, and transmission lines alone cover thousands of miles within California. UAVs could be used for rapid damage assessment as well as perimeter protection enhancement.

3.3.5. Natural Gas Interdependencies

Natural gas is a primary fuel for electricity generation in California. Natural gas storage and pipeline security could be a concern for contingency planners to ensure stability and reliability of electricity transmission.

3.4. Research Areas of Interest and Candidate Project Concepts

Following the individual interviews with stakeholders, the Security Research Program held a one-day roundtable at which the Candidate Research Initiatives were discussed.

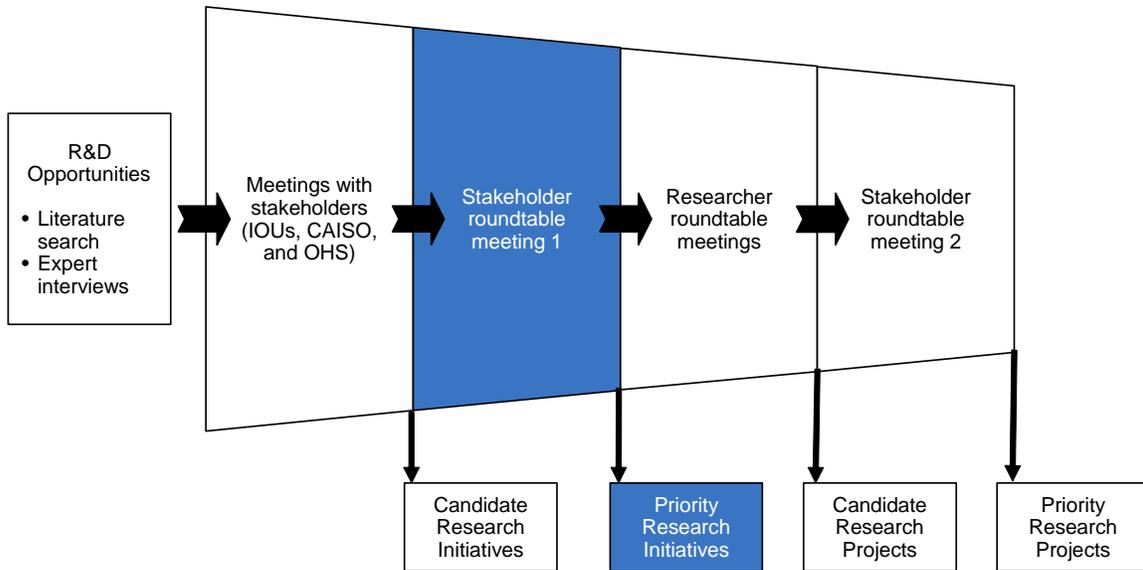


Figure 5: Stakeholder roundtable determines Priority Research Initiatives

Source: Security Research Program: Research Opportunity Assessment

For each Candidate Research Initiative, stakeholders were presented with a vulnerability and scope of potential impact that the initiative would address. Also presented were issues that might affect the vulnerability, impact or ability of the stakeholders to respond. The stakeholders were asked to identify and discuss potential research needs that could address the vulnerability, and finally recommend potential actions that the Security Research Program might undertake in response. Figure 6 displays the Priority Research Initiatives that were identified by the group.

Priority Research Initiatives	Illustrative Candidate Research Projects
Data Security for Non-Transmission Infrastructure and Emerging Technologies	Conduct a vulnerability assessment of substation and distribution data infrastructure and technologies
Technologies to Resist Physical Damage from Blasts and Bullets	Survey existing technology capability and adaptability to determine tech transfer opportunities
Unmanned Aerial Vehicles (UAVs)	Develop and demonstrate a utility application of the technology
Transportation Infrastructure	Determine the current base of information and develop a routing optimization model to meet utility needs
Emerging Technologies for Infrastructure Hardening	Further explore existing or emerging technologies and their application/adaptability
Sensors and Wireless Networks for Utility Security Applications	Further explore existing or emerging technologies and their application/adaptability

Researcher Roundtables

Figure 6: Priority Research Initiatives

Source: Security Research Program: Research Opportunity Assessment

For four of the six Priority Research Initiatives, the group of stakeholders was able to identify potential research activities for the Security Research Program. Given the nature of the “Emerging Technologies for Infrastructure Hardening” and “Sensors and Wireless Networks for Utility Security Applications” initiatives, it was determined that focused roundtables of technology experts were necessary for identifying potential future activities.

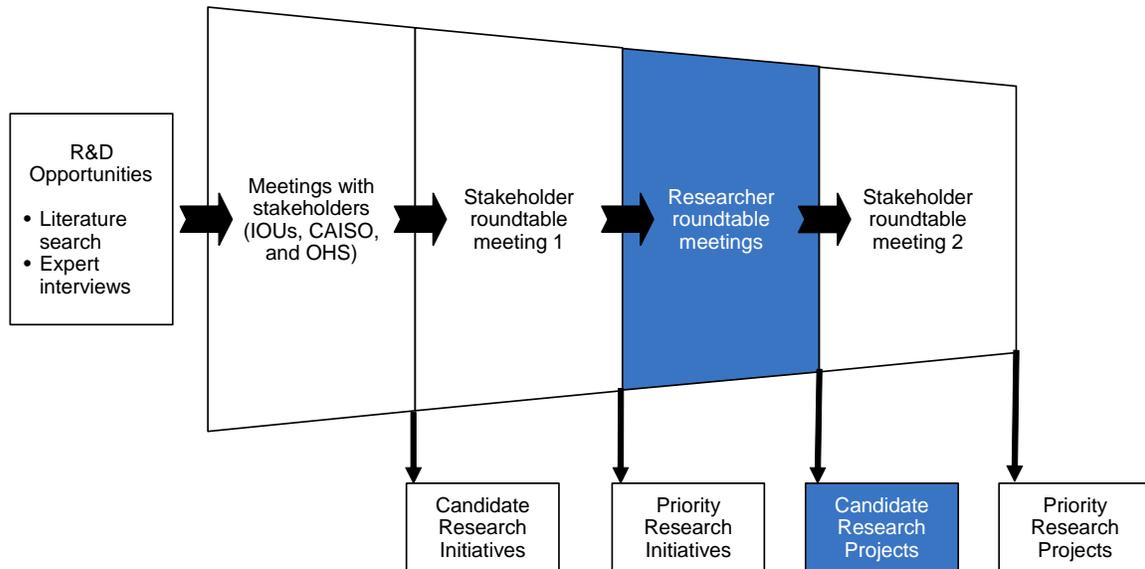


Figure 7: Researcher roundtables identify Candidate Research Projects

Source: Security Research Program: Research Opportunity Assessment

As part of the researcher roundtable meetings, world class technology experts were presented with key questions and challenges taken from discussions with stakeholders. These experts were asked to come up with potential solutions based on technologies that were available or emerging in the near term. In many cases these technologies had been developed for applications other than electric infrastructure, but were in need of refinement and demonstration in a utility application. Taking input from roundtable discussions with researchers, ten credible research project concepts emerged that address one of the six initiatives (see Appendix B for detailed descriptions of each candidate research project).

Candidate Research Projects		Research Area
(A)	Develop an advanced sensor network optimized for utility applications	Infrastructure Hardening
(B)	Develop a utility-customized sensor network algorithm	Infrastructure Hardening
(C)	Integrate different types of sensors for higher reliability	Infrastructure Hardening
(D)	Explore emerging technologies for enhanced data security below the transmission level	Cyber Security
(E)	Assess the feasibility of wireless network protection technologies	Cyber Security
(F)	Explore novel non-lethal techniques for denial of access	Infrastructure Hardening
(G)	Explore novel temporary armor system technologies	Infrastructure Hardening
(H)	Survey technologies to resist physical damage from blasts and bullets	Infrastructure Hardening
(I)	Develop transportation routing model for rapid system recovery	Interdependencies & Logistics
(J)	Explore the feasibility of deploying UAVs for utility applications	Interdependencies & Logistics

Figure 8: Candidate Research Projects

Source: Security Research Program: Research Opportunity Assessment

4.0 Identification of Policy Linkage and Project Scoping

4.1. Policy Linkage and Project Prioritization

The Priority Research Projects were selected from the list of projects created prior to the second stakeholder roundtable.

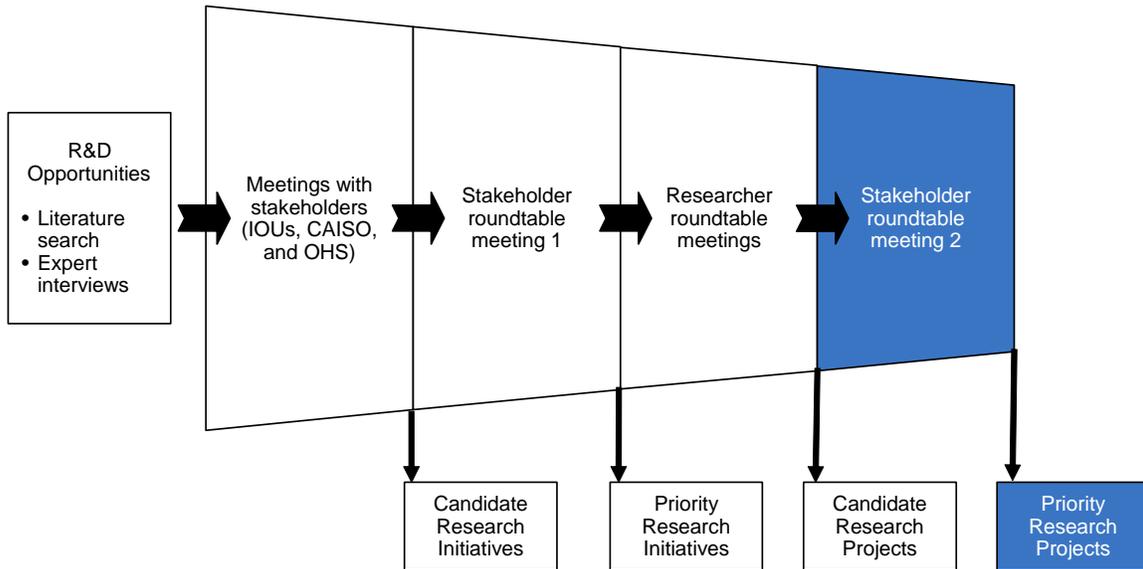


Figure 9: Stakeholder roundtable selects Priority Research Projects

Source: Security Research Program: Research Opportunity Assessment

The PIER's program, as it is funded by payments from IOU ratepayers, is mandated to perform researches with high level of public interest. For the Security Research Program in particular, the projects it takes on must also be valuable to key stakeholders, as the utilities, OHS, and the CAISO are important driving forces for demonstrating and deploying the products of the program's research (Figure 10). As such, the Security program refined the ten project concepts through identification of policy linkage and collection of feedback from key stakeholders. The program took the following three policy documents into consideration as it evaluated the strength of policy linkage.

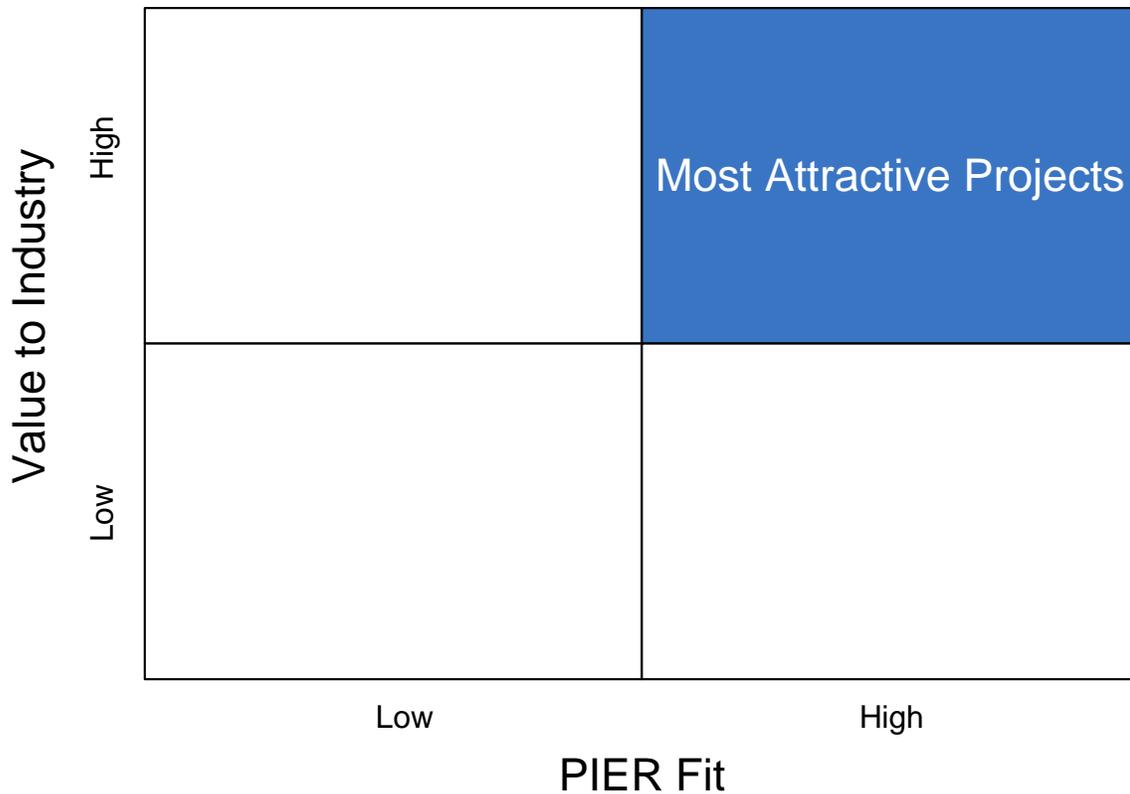


Figure 10: Prioritization Matrix Concept

Source: Security Research Program: Research Opportunity Assessment

4.1.1. 2007-2011 Electricity Research Investment Plan

In March 2006, the Energy Commission created the PIER Program 2007 – 2011 Electricity Research Investment Plan, setting forth a long-term research priority, program management, and staffing plan for the PIER program. The Plan identifies five key energy issues important to California, which are:

- Affordable, comfortable, and energy-smart choices for daily life and a strong California economy.
- Clean and diverse electricity supply that optimizes California’s resources.
- Clean and diverse transportation system in California.
- Integrated electric system that is reliable and secure.
- Environmentally sound electricity system in California.

The PIER Security Research Program’s efforts align particularly well with the fourth issue: “integrated electric system that is reliable and secure”. The Research Investment Plan identifies one of the objectives to be to “improve security and reliability of electricity system,” which “will address the increasing focus on energy security and protection against natural and terrorist threats to energy infrastructure.” One of the primary areas of R&D

listed under this issue is to “develop an electric system (cyber and physical) that is resilient to natural and man-made events, self-diagnosing, and self-healing.” The Plan identifies the benefit for the ratepayers to be “the increased reliability [that] will result from a modernized and secure electric transmission and distribution system that provides more energy options to the grid managers and recovers faster when unavoidable problems occur.”

4.1.2. Energy Action Plan

In September 2005, the California Public Utilities Commission and the Energy Commission jointly prepared Energy Action Plan II (EAP II), which identified the actions necessary to meet California’s future energy needs. This was prepared to support and expand the commitment to cooperation among state agencies embodied in the original EAP prepared in 2003.

EAP II identifies nine items as specific action areas⁴. The Security Research Program’s effort aligns with the “Electricity Adequacy, Reliability, and Infrastructure” area, in which EAP II declares that “an expanded, robust electric transmission system is required to... increase grid reliability,” and that “the distribution system, which has the most direct effect on reliable service for consumers, must be continually upgraded and reinforced.”

4.1.3. 2005 Integrated Energy Policy Report

In the fall of 2002, the California State Legislature passed Senate Bill 1389 [Chapter 568, Statutes of 2002, Bowen] requiring the California Energy Commission to prepare a biennial integrated energy policy report. In accordance with this Bill, the Energy Commission, California Public Utilities Commission and California Power Authority created their first version of Integrated Energy Policy Report (IEPR), creating a common vision to direct the future efforts at the three principal energy agencies.

The 2005 IEPR states in its executive summary; “The most critical [energy] infrastructure issue is the state’s electricity transmission system, which has become progressively stressed in recent years. The systematic under-investment in transmission infrastructure is reducing system reliability and increasing operational costs.” The effort at PIER Security Research Program is aimed to catalyze investment on the part of utility stakeholders to enhance security of their critical assets, and thus improving electricity system reliability while decreasing operational costs.

4.1.4. Key Applicable Passages of Policy Documents

The key passages of the policy documents applicable to the Security Research Program are as follows:

⁴ Specific action areas identified in EAP II are: Energy Efficiency; Demand Response; Renewables; Electricity Adequacy, Reliability, and Infrastructure; Electricity Market Structure; Natural Gas Supply, Demand, and Infrastructure; Transportation Fuel Supply, Demand and Infrastructure; Research, Development, and Demonstration; Climate Change.

- PIER Program 2007 – 2011 Electricity Research Investment Plan
 - “Improve security and reliability of electricity system. This objective will address the increasing focus on energy security and protection against natural and terrorist threats to energy infrastructure.” (Integrated Electricity System that is Reliable and Secure: Objective #4, p.28)
 - “Develop an electric system (cyber and physical) that is resilient to natural and man-made events, self-diagnosing, and self-healing.” (Integrated Electricity System that is Reliable and Secure: PIER Research Solutions, Primary Areas of RD&D, p.29)
 - “The increased reliability will result from a modernized and secure electric transmission and distribution system that provides more energy options to the grid managers and recovers faster when unavoidable problems occur.” (Integrated Electricity System that is Reliable and Secure: Benefits to Californians, p.30)

- State of California Energy Action Plan II
 - “An expanded, robust electric transmission system is required to... increase grid reliability.” (Specific Action Areas: Electricity Adequacy, Reliability and Infrastructure, p.7)
 - [T]he distribution system, which has the most direct effect on reliable service for consumers, must be continually upgraded and reinforced.” (Specific Action Areas: Electricity Adequacy, Reliability and Infrastructure, p.7)

- California Energy Commission 2005 Integrated Energy Policy Report
 - “The most critical [energy] infrastructure issue is the state’s electricity transmission system, which has become progressively stressed in recent years. The systematic under-investment in transmission infrastructure is reducing system reliability and increasing operational costs.” (p.1)

4.2. Research Project Scoping

The Security Research Program used these policy considerations to determine the PIER Fit of the ten project concepts described at the end of the previous chapter. Combining PIER Fit scores with the industry scores obtained at the key stakeholder roundtable (see Appendix B); project concepts were plotted on the prioritization matrix (Figure 11).

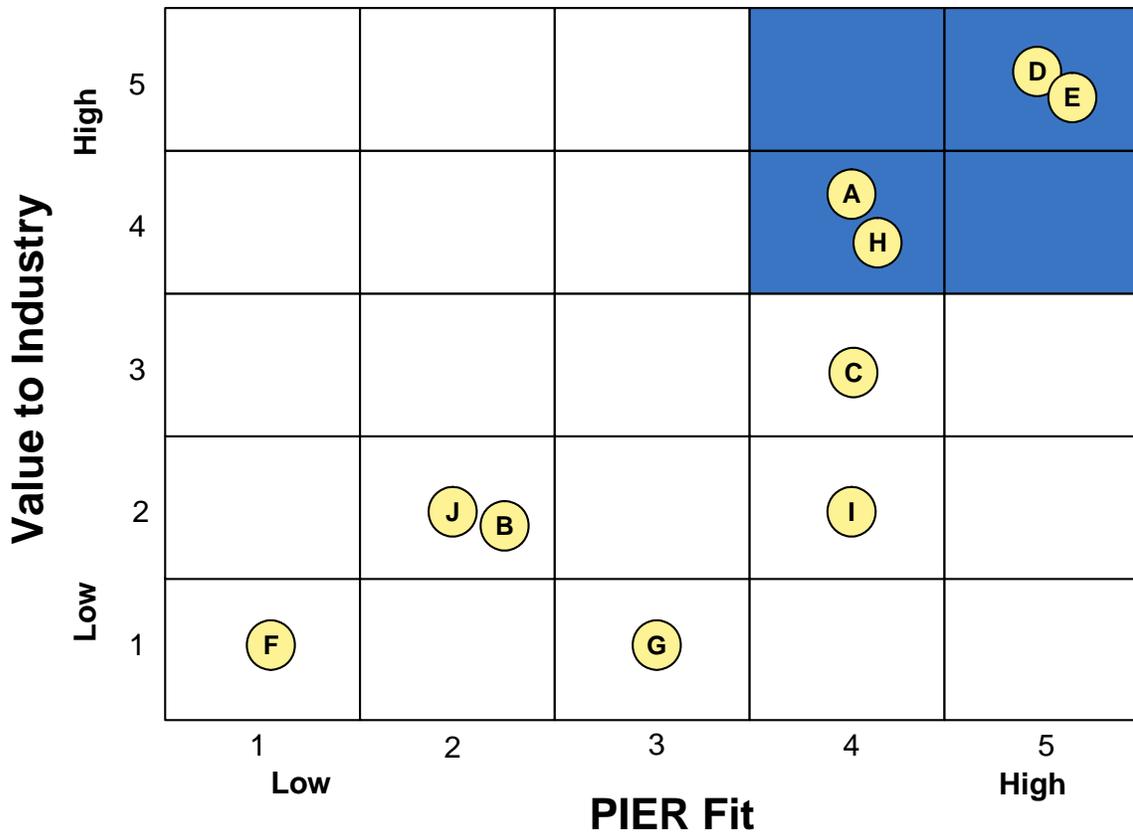


Figure 11: Project Prioritization Results

Source: Security Research Program: Research Opportunity Assessment

- A. Develop an advanced sensor network optimized for utility applications
- B. Develop a utility-customized sensor network algorithm
- C. Integrate different types of sensors for higher reliability
- D. Explore emerging technologies for enhanced data security below the transmission level
- E. Assess the feasibility of wireless network protection technologies
- F. Explore novel non-lethal techniques for denial of access
- G. Explore novel temporary armor system technologies
- H. Survey technologies to resist physical damage from blasts and bullets
- I. Develop transportation routing model for rapid system recovery
- J. Explore the feasibility of deploying UAVs for utility application

Based on their value to industry and fit with PIER objectives, project concepts A, D, E, and H were deemed to be the most valuable in the near term. Project A made it through the stakeholder discussion with minimal edits. Projects D and E were combined during the discussion and the scorings reflected an assumption that any future project would pursue elements of both project concepts simultaneously. Project concept H was broadened to consider natural threats as well as man-made threats.

Three high priority project concepts are scoped below:

- Project 1 (A): Develop an advanced distributed sensor network optimized for utility applications;
- Project 2 (D&E): Assess the feasibility of wireless technologies for enhanced data and network security below the transmission level; and
- Project 3 (H): Survey technologies to resist physical damage.

Project 1 (A). Develop an advanced distributed sensor network optimized for utility applications

Research Area

Infrastructure Hardening

Research Initiative

Sensors and Wireless Networks for Utility Security Applications

Stakeholder Input

“We have identified critical infrastructure, and we need a specific project and field test to deploy these monitors and relay the information back to the control center.”

“Some of these technologies are more mature than you may think. Most of them are the size of a coffee cup, and some of them have pattern recognition capability.”

“Advanced sensors could also pick up temperatures. The biggest threat for the grid today is wild fire. This would give us real information as to the proximity of the fire to the [transmission] line.”

Project Description

The researchers will design and develop an advanced sensor network optimized for utility applications employing the concept of dust networks, which is a network of wireless microelectromechanical system (MEMS) devices, or “motest”, equipped with sensors. False positive mitigation, data fusion, latency issues, power harvesting, cost reduction and deployment feasibility are some of the issues that must be addressed during the course of the project. The expected duration of the project is 18 months with an estimated budget of \$1.5 million. Research participants will include sensor network specialists from national laboratories, manufacturers of sensor hardware, and R&D integration firms with expertise in this area.

Project 2 (D&E). Assess the feasibility of wireless technologies for enhanced data and network security below the transmission level

Research Area

Cyber Security

Research Initiative

Data Security for Non-Transmission Infrastructure and Emerging Technologies

Stakeholder Input

“A project like this defines the problem. There are lots of data out there and we don’t know what the vulnerabilities are.”

“This is something that needs to be looked at. Everyone’s going wireless, but I’m not convinced that we have the best protection in place.”

Project Description

This project involves performing data security vulnerability assessment of technologies applied below the transmission level, such as distribution automation, phasor measurement units (PMUs) and distributed energy sources (DER). Since there is an increased interest among the utilities to employ wireless network technologies to operated tasks below the transmission level, this assessment should also cover vulnerabilities of wireless network technologies themselves.

This is a two-phase project. The first phase will be the feasibility study of applying and deploying the technologies for utility applications. The second phase will be demonstration, which will take place following the successful completion of the assessment. The expected duration of the overall project is 12 months. Estimated total budget is \$400,000, where \$150,000 will be allocated to Phase One, and the remaining \$250,000 to Phase Two. Various national laboratories have expertise in the relevant fields, and they will likely collaborate with hardware manufacturers as well as other wireless security experts to carry out this project.

Project 3 (H). Survey technologies to resist physical damage

Research Area

Infrastructure Hardening

Research Initiative

Technologies to Resist Physical Damages from Blasts and Bullets (expanded)

Stakeholder Input

“A specification document to support technology selection would be helpful.”

“There might be other applications in addition to security. We did our own assessment on something similar, mainly focusing on protection against fire.”

Project Description

This project will be a survey of existing technology options and their capability and adaptability characteristics for electricity infrastructure applications. The project partners will perform literature search to analyze gaps and opportunities for promising technologies to improve the survivability of key assets against natural disasters and human attacks. The expected duration of the project is 6 months, with the estimated budget of \$100,000. Defense contractors, T&D (transmission and distribution) and security suppliers will collaborate with utilities and researchers from national laboratories to expand their existing knowledge on this topic.

5.0 Next Steps

This research opportunity assessment identified opportunities for the PIER Security Research Program to pursue. While much work is underway to address security vulnerabilities for the electric power infrastructure in California, technology gaps exist that could be more quickly closed with focused R&D efforts supported by the program. As the program moves forward, it will strive to maintain and enhance its research portfolio to meet evolving security needs of California's key electricity stakeholders.

The Security Research Program portfolio will include a mix of projects that vary in size and timing, in order to maximize the value of the program's limited resources. To ensure that the program continues to address key stakeholder issues, regular surveys of the research landscape will be conducted to identify emerging technologies that might be relevant to the enhancement of electricity infrastructure security. In addition, the program will continue to engage in dialogue with key stakeholders to keep the program updated of changes in utility setting and security needs over time.

Another key issue for the program will be to ensure that its R&D results could be implemented in the electricity system effectively and efficiently. The program will continue to explore various implementation vehicles and partnership opportunities to maximize benefits to ratepayers.

Appendices

Appendix A: Public Interest Screening Criteria

The PIER program plays a key role in technology development and informing energy policy. PIER performs research that enables the development and market adoption of new energy technologies that respond to current energy policy and provide significant benefits to Californians. PIER also performs research that provides valuable input to policymakers regarding science and technology, resulting in enhanced and timely policy development, including research required to develop regulations, tariffs, and incentives. In addition, PIER performs research on emerging energy issues that will lead to the development of future state energy policy.

The PIER program is legislatively mandated to perform only public interest energy research. The legislation provides general guidance as to what should be considered public interest energy research (Figure A-1).

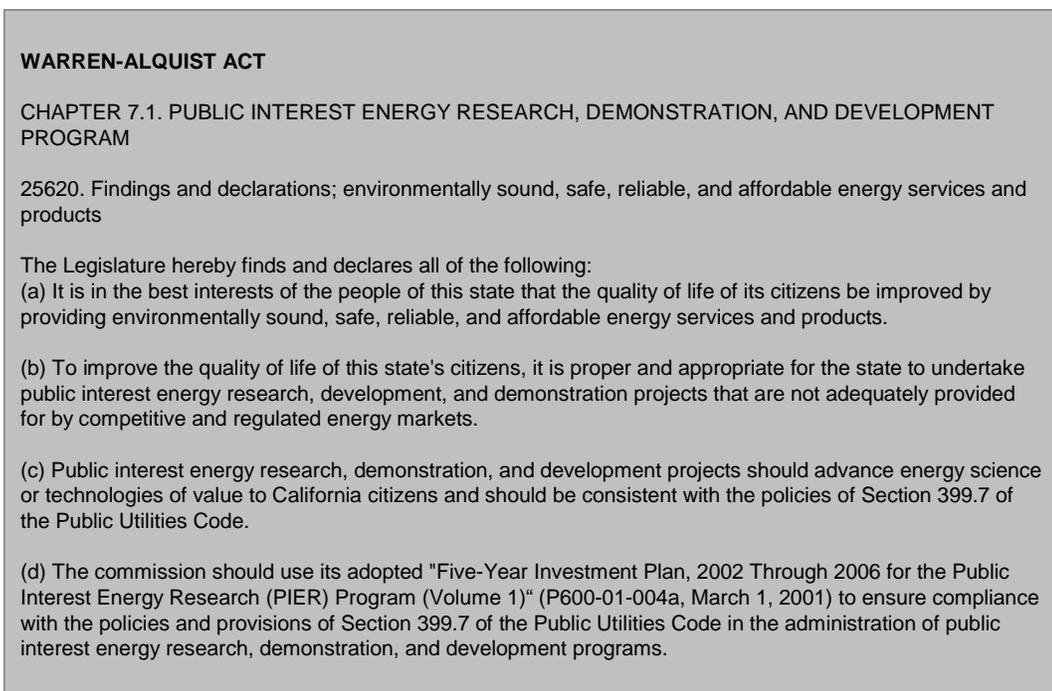
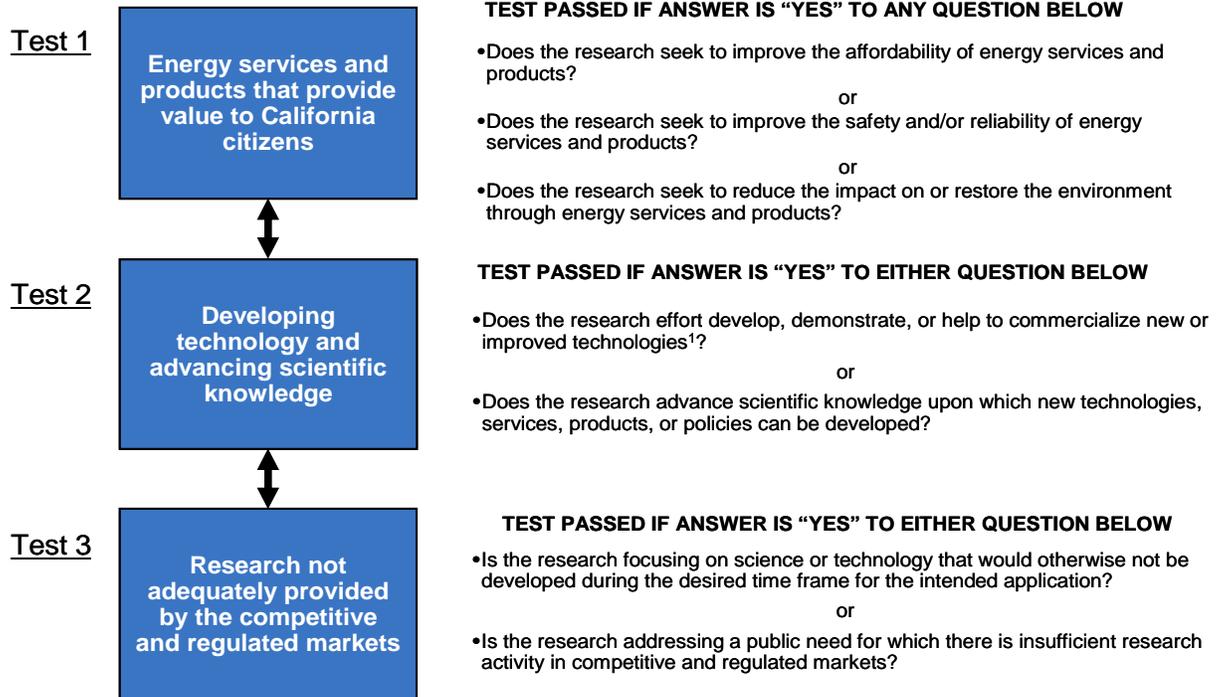


Figure A-1: Legislative Guidance on Public Interest Research

Source: Security Research Program: Research Opportunity Assessment

However, the PIER program requires a more specific set of criteria that could be used in selecting a wide range of potential projects across the different program areas. As a result, PIER has developed an improved set of criteria consistent with current PIER legislation to evaluate if a project meets the public interest mandate. As Figure A-2 shows, each proposed project needs to pass three tests to meet the public interest criteria and be eligible for PIER

funding. The public interest screening is the first step in the project selection process. If a proposed project meets the Public Interest Screening Criteria, it will then be evaluated against additional project selection criteria (such as alignment of the project with PIER’s strategic objectives, value to ratepayers, contribution to research roadmap as well as others) used by PIER program managers to select the best projects to fund.



¹Technology includes hardware, software, systems, exploratory concepts, and supporting knowledge.

Figure A-2: Public Interest Screening Criteria

Source: Security Research Program: Research Opportunity Assessment

Appendix B: Research Project Scoping

Based on the roundtable discussions with stakeholders and research community members, the Security Research program selected ten projects which project concept intersects with the policies discussed in the previous section.

Project A: Develop an advanced sensor network optimized for utility applications.

Research Initiative

Technologies to Resist Physical Damages from Blasts and Bullets (expanded)

Project Description

Design and develop an advanced sensor network (e.g., dust networks) optimized for utility applications. Issues to consider include false positive mitigation, data fusion, latency issues, and power harvesting. Also, hardware and deployment costs need to be reduced relative to options currently available for widespread deployment.

R&D Partners

Manufacturers, national labs, R&D integration firms

Timeframe

1.5 years

Budget Estimate

\$1.5 million

Value to the Industry

This project will advance the technology for utility applications in providing systems that will have reduced maintenance requirements and better address the specific needs of the electric utilities.

Pros :

- Mature technologies exist
- Broad security application (e.g. substation, transmission lines)
- Could offer operational benefits

Cons:

- Cost must be reduced
- False Positives
- Data integrity must be ensured

Score: 4

PIER Fit

Advanced sensor networks could significantly enhance the level of protection for facilities critical to electric service reliability. PIER could catalyze the transfer of these advanced technologies to the electric utility industry through this research.

Score: 4

Project B: Develop a utility-customized sensor network algorithm.

Project Description

Develop the algorithm and processor of a sensor network that are optimized for the specific sensors deemed valuable for electric utility security applications.

Research Initiative

Sensors and Wireless Networks for Utility Security Applications

R&D Partners

National labs (for algorithm development), manufacturers (for systems integration and product development)

Timeframe

1.5 years

Budget Estimate

\$500,000 to \$1 million

Value to the Industry

Sensor-specific algorithms will increase the reliability of the sensor network.

Pros:

- Reduces false positives

Cons:

- Communication logistics must be ironed out before considering security options
- Adaptability to new technologies down the road questionable

Score: 2

PIER Fit

Applicability beyond utility involved in this project may be limited. Project is not likely to have any long term impact.

Score: 2

Project C: Integrate different types of sensors for higher reliability.

Project Description

Integrate different types of sensors (e.g. smart CCTV, fiber optics) to reduce false positives; one type of sensor could adjust another sensor's alarming algorithm, or could serve to double-check. It could be coupled with signature recognition for higher efficiency and reliability.

Research Initiative

Sensors and Wireless Networks for Utility Security Applications

R&D Partners

National labs, universities, manufacturers

Timeframe

2 years

Budget Estimate

\$1 million

Value to the Industry

In addition to higher reliability, multiple sensor integration could allow the control room to better identify the nature of the threats.

Pros:

- Higher reliability of the sensor system as a whole (i.e. failure of one sensor will not significantly affect the system)
- Reduces false positives
- Could reduce number of guards at security centers

Cons:

- Does not require immediate attention
- May duplicate similar efforts by private sector entities

Score: 4

PIER Fit

Cost-effective and reliable security is beneficial to asset owners and ratepayers. This is a technology transfer opportunity for application specific to energy infrastructure.

Score: 3

Project D: Explore emerging technologies for enhanced data security at the sub-transmission level.

Project Description

Perform data security vulnerability assessment of technologies such as distribution automation, phasor measurement units (PMUs) and distributed energy sources (DER). Identify appropriate emerging technologies that could address these vulnerabilities.

Research Initiative

Data Security for Non-Transmission Infrastructure and Emerging Technologies

R&D Partners

National labs

Timeframe

1 year

Budget Estimate

\$200,000

Value to the Industry

Reduced the threat of attack through sub-transmission level data networks will improve operational stability of the electricity system.

Pros:

- Provides better understanding of system vulnerabilities
- Provides additional protection for field devices (e.g. sensors, AMI devices)

Cons:

- Maintainability of the technologies questionable

Score: 5

PIER Fit

Data management is critical for reliable operation of the grid. Increased data security could improve electricity service reliability for ratepayers.

Score: 4

Project E: Assess the feasibility of wireless network protection technologies.

Project Description

Examine existing technologies for wireless network protection, and study the feasibility of applying the technologies for utility applications. Demonstrations will take place following the successful completion of the assessment.

Research Initiative

Data Security for Non-Transmission Infrastructure

R&D Partners

Manufacturers, national labs, wireless security experts

Timeframe

1 year

Budget Estimate

Feasibility Assessment: \$100,000

Demonstration: \$200,000

Value to the Industry

Improving the security of wireless networks will serve as a preemptive measure to protect against cyber attacks (e.g. denial of service) as the systems are gradually introduced.

Pros:

- Facilitates secure applications of wireless technologies
- Broad applications throughout the electricity system (e.g. distribution level)

Cons:

- Extra consideration for data security is necessary

Score: 5

PIER Fit

Wireless networks can potentially enhance the level of protection at reduced cost relative to wired data networks. However, data security is currently a significant obstacle to widespread implementation. There is potential for long term impact through research in this area.

Score: 5

Project F: Explore novel non-lethal techniques for denial of access.

Project Description

Perform “bake-off” to assess performance of non-lethal protection measures (e.g. sticky foam, pepper balls, sonic standoff). Perform feasibility assessment of the technologies, given their performance and associated potential collateral damage on the assets.

Research Initiative

Emerging Technologies for Infrastructure Hardening

R&D Partners

National labs

Timeframe

1 year

Budget Estimate

“Bake-off”: \$150,000

Feasibility Assessment: \$1 million

Value to the Industry

Non-lethal access denial technologies will provide an effective secondary or tertiary protection layer around critical facilities not currently available.

Pros:

- Could offer an alternate system security “posture” between business-as-usual state and state of heightened alert
- Could serve as a device to warn non-malicious intruders

Cons:

- Considerable liability issues
- Environmental concerns associated with some technologies

Score: 1

PIER Fit

Potentially controversial use of program funds with significant downside risk.

Score: 1

Project G: Explore novel temporary armor system technologies.

Project Description

Examine the feasibility of applying existing temporary armor system technologies (e.g. blanket) for utility settings. Key attributes sought include low cost and simple, rapid assembly.

Research Initiative

Emerging Technologies for Infrastructure Hardening

R&D Partners

National labs, equipment manufacturers, DoD protection systems providers (e.g., Kevlar and light armor manufacturers)

Timeframe

0.5 year

Budget Estimate

\$250,000

Value to the Industry

Temporary armor technologies will provide a cost-effective means to protect critical physical assets during periods of heightened threat levels.

Pros:

- No thermal overhead
- Knowledge exist with military forces

Cons:

- Deployment issues
- Requires personnel to deploy the system
- Military resources exist for temporary protection of assets

Score: 1

PIER Fit

The ability to quickly respond to impending threats through enhanced survivability and protection on an as-needed basis could enhance the resiliency of the system at a reasonable cost.

Score: 3

Project H: Survey technologies to resist physical damage from blasts and bullets.

Project Description

Conduct a survey of existing technology options and their capability and adaptability characteristics for electricity infrastructure applications.

Research Initiative

Technologies to Resist Physical Damages from Blasts and Bullets

R&D Partners

T&D and security suppliers, defense contractors, national labs

Timeframe

0.5 year

Budget Estimate

\$100,000

Value to the Industry

This survey will provide utilities with an enhanced understanding of available options for improving durability of assets against malicious man-made attacks.

Pros:

- Can easily expand to broader application (e.g. man-made events and natural disasters)
- Enhances the knowledge that exists among utilities

Cons:

- Budget must be reduced
- Does not consider structural weak points of critical assets

Score: 4

PIER Fit

Some elements of the electricity infrastructure are potential high-profile targets for attack. If the analysis were broadened out to include other man-made threats and natural disasters, the value of this effort would be further magnified. This analysis will identify options for enhancing protection of key electric system resources at reasonable cost.

Score: 4

Project I: Develop transportation routing model for rapid system recovery.

Project Description

Enhance the understanding of the transportation routing options currently available for the development of optimized emergency response plans.

Research Initiative

CalTrans, universities, CREATE, DOE, TSWG, PIER Transportation

R&D Partners

Transportation Infrastructure

Timeframe

1 year

Budget Estimate

\$250,000

Value to the Industry

Securing transportation routes for logistics surrounding repairs and spare deliveries would enhance the rapid recovery of the electricity system.

Pros:

- Speeds up the recovery process
- Could fill gaps among fragmental works done in this area

Cons:

- Project details must be refined to consider all tie-ins

Score: 3

PIER Fit

Rapid recovery of the electricity system reduces duration of outages following attack or failure of critical systems. Project has impacts beyond electricity and may interest other homeland security stakeholders. However, this project may involve the handling of sensitive information.

Score: 4

Project J: Explore the feasibility of deploying UAVs for utility applications.

Project Description

Examine, develop and demonstrate the utility application of Unmanned Aerial Vehicles (UAVs) for damage assessment and threat analysis.

Research Initiative

Unmanned Aerial Vehicles (UAVs)

R&D Partners

UAV suppliers, national labs, FAA

Timeframe

0.5 year

Budget Estimate

\$200,000

Value to the Industry

UAVs could be used for rapid damage assessment as well as perimeter protection enhancement.

Pros:

- Effective for line flydowns
- No personnel hazards in case of accidents
- No weather restrictions

Cons:

- Regulatory barriers
- Other comparable technologies (e.g. satellite imaging) exist
- Detracts from security (more geared toward recovery support)

Score: 2

PIER Fit

Rapid recovery of the electricity system reduces duration of outages following attack or failure of critical systems. However, there are significant regulatory roadblocks to using UAVs in California.

Score: 2