

Title of Proposed Initiative: Preventing Zero Day Attacks at Electric Utilities

Investment Areas (Check one or more):

- Applied Research and Development
- Technology Demonstration and Deployment
- Market Facilitation

Electricity System Value Chain (Check only one):

- Grid operations/market design
- Generation
- Transmission
- Distribution
- Demand-side management

Issues and Barriers:

As industrial control systems (ICS) at utilities incorporate digital technology, adopt standard protocols and platforms, connect with commodity information technology systems and the Internet, and rely more on wireless communication networks, they become more vulnerable to cyber-threats. The nature of these threats, methods to detect them, and appropriate protocols for addressing them are inadequately understood. “Zero Day” attacks that exploit a previously unknown vulnerability are of particular concern.

Initiative Description and Purpose:

This initiative would provide funding to further develop and test intrusion detection technologies to accelerate technology commercialization. Specifically, the initiative would develop a threat detection framework that enables utilities to protect their control systems from cyber attacks at the network, host, and device levels. The integrated solution will complement traditional, signature-based detection with multiple detection algorithms including model-based and flow anomaly detection and cross-site attack correlation.

Unlike corporate IT systems, which may be able to shut down during an attack, utilities must continue to provide service. Utilities need new defense mechanisms that are ICS-specific and that complement traditional enterprise security solutions.

Stakeholders:

Ratepayers, utility operators, electricity users, and organizations developing new intrusion detection systems would benefit from this initiative.

Background and the State-of-the-Art:

Since 2010, the Department of Energy has invested more than \$100 million in cybersecurity research and development through awards and funding provided to industry, universities and national laboratories (<http://energy.gov/articles/energy-department-announces-new-investments->

EPIC TRIENNIAL INVESTMENT PLAN 2015-17**Proposed Energy Research Initiative****Questionnaire**

CALIFORNIA ENERGY COMMISSION

over-30-million-better-protect-nation-s). In addition, agencies such as the Department of Homeland Security also support energy-related cyber security research (<http://www.dhs.gov/science-and-technology-directorate-cyber-security-division>). However, funding to test these new technologies against real-world problems faced by utilities is inadequate. Funding for testing would enable California companies developing new solutions to confirm that their new concepts address utility needs and support the commercialization of emerging technologies.

Justification:

In fiscal year 2012, the U.S. Department of Homeland Security's INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM (ICS-CERT) responded to 198 cyber incidents across all critical infrastructure sectors. Of these, 41% were in the energy sector. In the first half of fiscal year 2013, (October 1, 2012–May 2013), ICS-CERT responded to over 200 incidents across all critical infrastructure sectors, with the highest percentage of incidents (53%) occurring in the energy sector (https://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf).

As stated in ICS-CERT's April-June Monitor, "the ability to detect anomalous network activity and network intrusions early in an incident greatly increases the chance of a successful mitigation and resolution." According to a 2012 study from the Ponemon Institute (*Cost of Cyber Crime Study: United States, Benchmark Study of U.S. Companies*, October 2012), the average annual cost of cyberattacks in U.S. Utilities & Energy sector: \$20M per company.

Ratepayer Benefits (Check one or more):

- Promote greater reliability
- Potential energy and cost savings
- Increased safety
- Societal benefits
- Environmental benefits - specify
- GHG emissions mitigation/adaptation in the electricity sector at the lowest possible cost
- Low emission vehicles/transportation
- Waste reduction
- Economic development

Describe specific benefits (qualitative and quantitative) of the proposed initiative:
Reliable infrastructure.

Public Utilities Code Sections 740.1 and 8360:

Please describe how this technology or strategy addresses the principles articulated in California Public Utilities Code Sections 740.1 and 8360. The California Public Utilities Code is available online at www.leginfo.ca.gov/cgi-bin/calawquery?codesection=puc.

EPIC TRIENNIAL INVESTMENT PLAN 2015-17

Proposed Energy Research Initiative

Questionnaire

CALIFORNIA ENERGY COMMISSION

This project offers a strong probability of providing benefits to ratepayers. Cyber threats are real and evolve continuously. Current methods for detecting “zero day” attacks are inadequate, but new intrusion detection systems under development show promise and should be tested against real data in a protected environment/test bed. This project would specifically address goals to improve public and employee safety, improve operating efficiency and reliability, and to reduce operating costs.

This project is also consistent with the state’s policy to modernize the state's electrical transmission and distribution system to maintain safe, reliable, efficient, and secure electrical service, with infrastructure that can meet future growth in demand and achieve all of the following, which together characterize a smart grid. Specifically, the project would promote the following objectives:

- (a) Increased use of cost-effective digital information and control technology to improve reliability, security, and efficiency of the electric grid.
- (b) Dynamic optimization of grid operations and resources, including appropriate consideration for asset management and utilization of related grid operations and resources, with cost-effective full cyber security.