# Fact Sheet: DOE Award Selections for the Development of Next Generation Cybersecurity Technologies and Tools

On September 12, 2017, the Department of Energy (DOE) announced the award of over $20 million to DOE's National Laboratories and partners to support critical early stage research and development of next-generation tools, technologies, as well as building capacity throughout the energy sector for day-to-day operations such as cyber-threat information sharing, to strengthen protection of the Nation's electric grid and oil and gas infrastructure from the cyber threat.

The 20 projects supported by this funding will enhance the reliability and resilience of the Nation's energy critical infrastructure through innovative, scalable, and cost-effective research and development of cybersecurity solutions and operational capabilities. These technologies are expected to have broad applicability to the U.S. energy delivery sector by meeting their needs in a cost-effective manner with a clear path for acceptance by asset owners and operators.

There are six topic areas for the projects:

- Partnerships to reduce risk through vulnerability mitigation;
- Identify energy delivery system (EDS) equipment inadvertently exposed to the public internet to reduce the cybersecurity risk on the operational technology (OT) infrastructure;
- Energy delivery systems that can adapt to survive a cyber-incident;
- Energy delivery systems with verifiable trustworthiness;
- Cybersecure communications for operating resilient grid architectures; and
- Tools and technologies that enhance cybersecurity in the energy sector.

Below are details about the award recipients and the projects.

**NATIONAL LABORATORY AWARD RECIPIENTS**

| ACRONYM | FULL NAME | LOCATION |
|---|---|---|
| ANL | Argonne National Laboratory | Argonne, IL |
| INL | Idaho National Laboratory | Idaho Falls, ID |
| LBNL | Lawrence Berkeley National Laboratory | Berkeley, CA |
| LLNL | Lawrence Livermore National Laboratory | Livermore, CA |
| LANL | Los Alamos National Laboratory | Los Alamos, NM |
| NREL | National Renewable Energy Laboratory | Golden, CO |
| ORNL | Oak Ridge National Laboratory | Oak Ridge, TN |
| PNNL | Pacific Northwest National Laboratory | Richland, WA |
| SNL | Sandia National Laboratories | Albuquerque, NM |

| National Lab | Project Partners | Project Title | Project Description |
|---|---|---|---|
| ANL | Illinois Institute of Technology, Southern Methodist University, Commonwealth Edison, PJM Interconnection, USARMY RDECOM CERDEC, Eaton | Next-Generation Attack-Resilient Electricity Distribution Systems | Develop a cyber-attack-resilient architecture for next-generation electricity distribution systems that increase reliability by using distributed energy resources (DER) and microgrids. |
| INL | New Context (NC), Southern California Edison (SCE), PNNL, Iowa State University, Department of Defense (DoD) Air Force Fellows | (FIT) Firmware Indicator Translation | Develop techniques to translate indicators of compromise that may have initially been developed for use by IT desk-top systems, so they can be more effectively used for OT operational networks to help secure firmware on the embedded systems used by energy sector field devices. |
| LBNL | OSISoft, SunSpec Alliance, SolarEdge, HDPV Alliance, Power Standards Laboratory (PSL), Arizona State University, Siemens, National Rural Electric Cooperative Association (NRECA), Sacramento Municipal Utility District (SMUD), Con Edison | Adaptive Control of Electric Grid Components for Cyber-Resiliency | Enable distribution grids to adapt to resist a cyber-attack by (1) developing adaptive control algorithms for DER, voltage regulation, and protection systems; (2) analyze new attack scenarios and develop associated defensive strategies. |
| LLNL | Hawaiian Electric Company (HECO), Rochester Public Utilities, Eaton, SolarEdge, OSISoft, SGS, PSL | Cyber Interconnection Analysis for High Penetration of DER | Develop a tool that can evaluate cyber-risk, and design remediation strategies to survive a cyber-attack, for a distribution-level power grid that uses a high penetration of DER to enhance reliability. |

| National Lab | Project Partners | Project Title | Project Description |
|---|---|---|---|
| LLNL | San Diego Gas & Electric (SDG&E), PSL | GPS Interference Detection | Develop a technology to rapidly detect interference of precise synchronized time signals used by phasor measurement units (PMUs) for wide area situational awareness of power grid operations. |
| LLNL | Sempra Energy, SDG&E, Automatak, Schweitzer Engineering Laboratories (SEL) | Secure SCADA Protocol Characterization and Standardization | Advance SSP21 (Secure SCADA Protocol for the 21st Century) through development of an industrial key infrastructure (IKI) to help protect energy infrastructure information by easing the process of cryptographic key exchange. |
| LANL | ORNL | Quantum Key Distribution for the Energy Sector: Trusted Node Relays and Networks | Research, design and prototype a quantum secure communication (QSC) operational network, including trustworthy relays to extend distance and decrease cost, for critical energy infrastructure. |
| NREL | SNL, SEL, Public Service Company of New Mexico (PNM) Resources | (Module-OT) Modular Security Apparatus for Managing Distributed Cryptography for Command & Control Messages on Operational Technology (OT) Networks | Develop a lower-cost distributed cryptography technique to help protect energy infrastructure information, in particular, the operational networks used for command and control of DER that are being increasingly used to enhance power grid reliability. |
| ORNL | LLNL, LANL, SNL, Virginia Tech, University of Tennessee, University of Puerto Rico, CenterPoint, Commonwealth Edison, Con Edison, Duke Energy, Entergy, EPB, NRECA, NV Energy, Puerto Rico Electric Power Authority (PREPA), SMUD, | DarkNet | Define the requirements for a secure energy delivery control system network that is independent of the public internet, and uses existing but currently unused optical fiber, so called “dark fiber”. |

| National Lab | Project Partners | Project Title | Project Description |
|---|---|---|---|
| | SDG&E, Southern California Edison (SCE), Southern Company, Tennessee Valley Authority (TVA) | | |
| ORNL | LANL | Quantum Physics Secured Communications for the Energy Sector | Decrease cost, and increase distance, of Quantum Key Distribution systems that enable real-time detection of adversarial intrusion on control system networks. |
| ORNL | NRECA, Schneider Electric, ISA Security Compliance Institute, TVA, EPB | Energy Delivery Systems with Verifiable Trustworthiness | Provide a tool to verify the integrity of firmware used in energy delivery system devices, without taking the equipment offline. |
| ORNL | University of Illinois, University of Tennessee, University of Nebraska, Schneider Electric, Brixon | Malware Operational Mitigation (MOM) | Work with energy sector partners to mitigate cyber-risk in energy delivery systems and components. |
| PNNL | Guardtime, Washington State University, TVA, Siemens, DoD Homeland Defense and Security Information Analysis Center (HDIAC) | KISS (Keyless Infrastructure Security Solution) | Develop block-chain cybersecurity technology for distributed energy resources at the grid's edge, such as transactive energy exchanges that can be expected to create new markets. |
| PNNL | Shodan LLC, NRECA, Tenable Network Security, Chelan PUD | MEEDS (Mitigation of External-exposure of Energy Delivery System Equipment) | Develop a tool for use by a utility or energy asset owner/operator, to identify their energy delivery system equipment that may have been inadvertently exposed to the public internet and mitigate associated risk. |
| PNNL | Tenable Network Security, Chelan County Public Utility District, University of Illinois, NRECA | SASS-E (Safe & Secure Autonomous Scanning Solution for Energy Delivery Systems) | Develop scanning methodologies, models, and architectures to transform a network vulnerability scanner widely deployed in the IT space, into a scanner that can be used in the operational |

| National Lab | Project Partners | Project Title | Project Description |
|---|---|---|---|
| | | | technology (OT) networks of critical energy infrastructure where legacy equipment may respond unpredictably when subjected to active scanning techniques often used in IT. |
| PNNL | Dispersive Technologies, California Independent System Operator (CAISO), Juniper, SEL, SCE, United States Pacific Command (PACOM), United States Northern Command (NORTHCOM), United States Cyber Command (CyberCOM), SNL | SDN4EDS (Software Defined Networking for Energy Delivery Systems) | Develop a comprehensive blueprint and secure reference architecture to ease the process of deploying software defined networking (SDN) technology to better secure operational networks throughout the energy sector. |
| PNNL | Open Access Technology International, Inc. (OATI), MITRE, Western Area Power Administration (WAPA) | UUDEX (Universal Utility Data Exchange) | Develop a secure and flexible data exchange approach for communication between control centers, including Inter-Control Center Communications Protocol (ICCP) data exchanges. |
| PNNL | Siemens, Minnesota Valley Electric Coop, South River Electric Membership Coop, Soteria | VERITAS (Vulnerability, Exploit, and Risk Identification Toolset and Source) | Build partnership among suppliers and end users of energy delivery infrastructure components and systems to reduce cyber-risk. |
| SNL | SEL, Chevron, Sempra Energy Utilities, Grimm, Ft. Belvoir, PNNL | Containerized Application Security for Industrial Control Systems | This project will increase the availability and resiliency of control systems by dynamically migrating, updating and restoring applications during a cyber incident. |

| National Lab | Project Partners | Project Title | Project Description |
|---|---|---|---|
| SNL | GT, PNNL, Grimm, SEL, Chevron, Sempra Energy Utilities, Ft. Belvoir | Survivable ICS | This project will develop technology that proactively detects adversarial manipulation of power system equipment by, for example, checking that received commands support grid stability, and appropriately respond by, for example, reconfiguring the operational network to isolate, then eradicate, the intrusion while sustaining critical energy delivery functions. |