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

As part of the Obama Administration's commitment to protecting America's energy critical infrastructure, the Department of Energy (DOE) announced up to $34 million in funding, subject to appropriations, for twelve projects representing energy sector organizations in nine states through the Office of Electricity Delivery and Energy Reliability's Cybersecurity of Energy Delivery Systems (CEDS) program.

The twelve projects will enhance the reliability and resilience of the nation's energy critical infrastructure through innovative, scalable, and cost-effective research, development and demonstration of cybersecurity solutions. These technologies are expected to have broad applicability to the U.S. energy delivery sector by meeting the needs of the energy sector in a cost-effective manner with a clear path for acceptance by asset owners and operators and through commercialization by solution providers.

There are five topic areas for projects**:**

- **Topic Area 1**: "Detect Adversarial Manipulation of Energy Delivery Systems Components" – The focus is the ability to detect and respond to cyberattacks designed to avoid detection by exploiting routine operations normally performed by energy delivery systems.
- **Topic Area 2**: "Secure Integration of Renewable Energy and Energy Efficiency Resources" – The focus is on making the integration of renewables onto the power grid at the generation, transmission and/or distribution levels more secure from cyber attacks. This may include the nexus of building control systems or plug-in hybrid vehicles with the power grid.
- **Topic Area 3**: "Continual and Autonomous Reduction of Cyber Attack Surface for Energy Delivery Control Systems" – The focus is on reducing exposures of energy delivery systems to cyber attacks, thereby making the systems more secure.
- **Topic Area 4**: "Supply Chain Cybersecurity for Energy Delivery Systems" – The focus is on detecting hostile hardware, firmware (combination of hardware and software), and/or software introduced at some point during the manufacture of energy delivery systems.
- **Topic Area 5**: "Innovative Technologies That Enhance Cybersecurity in the Energy Sector" – The focus will be on identifying gaps in the *Roadmap to Achieve Energy Delivery Systems Cybersecurity* and proposing innovative technical solutions to the identified risk. The twelve projects selected for awards are outlined below.

ABB, Inc. – Cary, NC
Topic Area 1
ABB will develop a security domain layer system that enables power systems to defend themselves against hacker and insider attacks that aim to disrupt electric power service.

ABB, Inc. – Cary, NC

Topic Area 2
ABB will research and demonstrate a cyber-physical control and protection architecture for the secure integration of multi-microgrid systems that can maintain stable performance during disruptive events such as cyber attacks.

Cyabti – Bloomington, IL
Topic Area 5
Cybati will develop a cybersecurity educational program on energy delivery systems that targets energy sector professionals, and college and high school students. The program will greatly simplify the educational constraints of a physical laboratory setup, cyber-engineering demonstration, and simulated scenario needed for users to build, break, and secure control systems by using kinetic models, software-defined networking, and virtualized industrial devices.

General Electric Company – Niskayuna, NY
Topic Area 5
GE will develop and demonstrate an automatic cyberattack anomaly detection and accommodation (ADA) system for power plants that will detect and respond to cyber-disruptions caused by cyber-attacks, and attacks against the cyber-physical interface. The system will localize where an attack occurred at critical interfaces and accommodate the system by maintaining uninterrupted operation in normal or degraded condition.

Intel Federal, LLC – Fairfax, VA
Topic Area 3
Intel will develop a security architecture solution to securely connect energy infrastructure devices to the cloud to allow the devices to interact with each other. Intel will demonstrate that the cyber-attack surface of energy delivery control systems can be continuously and autonomously reduced in a way that does not impede normal critical energy delivery functions.

Iowa State University – Ames, IA
Topic Area 3
Iowa State University will develop a comprehensive framework that continually assesses and autonomously reduces the attack surface for the power grid control environment by spanning substations, the control center, and the SCADA network to significantly reduce the risk of cyber-attacks.

National Rural Electric Cooperative Association (NRECA) – Arlington, VA
Topic Area 1
NRECA will develop and demonstrate technology for the rapid identification of anomalies in electric utility control communications as an indicator of cyber compromise to support expedited remediation by utility operators.

Qubitekk, Inc. – Bakersfield, CA
Topic Area 5
Qubitekk will advance an innovative technology that will enable multiple devices to communicate in a network that is more secure from eavesdropping and computing attacks.

Schweitzer Engineering Laboratories, Inc. – Pullman, WA
Topic Area 3
Schweitzer will develop a technology that will detect adversarial manipulation of energy delivery control systems by allowing control system operators to automatically identify undesired behavior, contain the affected network areas, and re-route critical information to keep systems operational.

Schweitzer Engineering Laboratories, Inc. – Pullman, WA
Topic Area 1
Schweitzer will develop algorithms and electronics to further strengthen cybersecurity of precise synchronized timing used in energy delivery.

Texas A&M University Engineering Experiment Station – College Station, TX
Topic Area 1
Texas A&M will develop detection methods and tools to further strengthen cybersecurity of precise synchronized timing to help ensure the resiliency of synchrophasor applications and legacy energy management systems.

United Technologies Research Center – East Hartford, CT
Topic Area 2
UTRC will develop an open-source, advanced cybersecurity platform that uses machine learning to more securely integrate legacy and emerging behind-the-meter Distributed Energy Resources (DERs).

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu