Topic Area #3: Development of Tools and Technology for Energy Cyber and Cyber-Physical Security in Critical Infrastructure

Note: For complete submission information see:
https://us-isr-energycenter.org/cfp/

Applicant submissions must include plans for the development and/or demonstration of newly developed cybersecurity technology or tool at a relevant end-user site to validate a clear path to industry acceptance. Selected applications will involve advanced tools technologies that are interoperable, scalable, and readily manageable. They will also include a strategy for transitioning solutions into practice throughout the energy sector through commercialization or by making the solution available through open source.

Development of Tools and Technologies

Proposals must describe R&D to deliver game-changing tools and technologies that help companies secure today's energy infrastructure from advanced cyber threats. Design next-generation future systems that are built from the start to collectively cooperate and interoperate in order to automatically detect, identify, reject, and withstand cyber incidents, regardless of the threat. Pursue enhancements to the reliability, survivability and resiliency of energy infrastructure, while addressing the relevant regulatory groundwork (e.g. concerning privacy etc.). All solutions must support current logging standards, ready to feed Big Data and Machine Learning based analytics systems.

Subtopics may include:

- Cyber secure cloud-based technologies for Operation Technology (OT) environment to facilitate threat sharing and automated defenses throughout the energy sector;
- Innovative technologies that enhance cybersecurity of OT environments in the energy sector though automated detection, identification and mitigation of cyber threats;
- Redesign for cyber-resilient architecture for the energy sector providing the ability for systems interoperate, communicate, and cooperate in order to continue to operate in their designed capacity before, during and after a cyber-incident;
- Ways and methods of accelerating the training phase and increase the accuracy of anomaly detection systems by using open-source knowledge of OT environments and architecture;
- Adversarial AI mitigation in Energy related systems;
- Utilizing 5G for a secure E2E implementation;
- Next Generation PLC cybersecurity;
- Secured edge Computing in the Energy Sector;
- Viable deception implementation in the Energy Sector;
- Time/Clock/GPS spoofing protection

Use of Tools and Technology

Strengthen the energy sector’s cybersecurity posture by leveraging and demonstrating already developed and vetted tools, guidelines, outreach, training and technical assistance in novel and improved ways, including the utilization of novel simulators.

Cyber Emergency Preparedness and Response

Pursue enhancements to the reliability, survivability and resiliency of energy infrastructure.
Facilitate faster recovery from disruptions to energy supply, including management and oversight of petroleum reserves.

Note: For complete submission information see:
https://us-isr-energycenter.org/cfp/