SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Cybersecurity for Energy Delivery Systems: What We Learned from DOE

Qinghua Li

University of Arkansas

September 15, 2017

Carnegie Mellon University
Electrical & Computer Engineering

University of Arkansas at Little Rock

University of Arkansas

Electric Cooperatives of Arkansas
Your Local Energy Partners

Lehigh University

MIT

FIU Florida International University

Outline

- **Involvement in DOE-funded research**
  - **Cybersecurity Center on Secure, Evolvable Energy Delivery Systems (SEEDS)**
- **DOE viewpoints that we as investigators observed**

SEEDS Overview

Cybersecurity for Energy Delivery Systems

Objective

- **Research and develop cybersecurity technologies, tools, and methodologies that will advance the energy sector's ability to survive cyber attacks and incidents while sustaining critical functions**

Basics

- **Funded by DOE/DHS**
- **Project start/end dates: 10/01/2015 – 09/30/2020**
- **Deliverables: cybersecurity technologies delivered multiple phases**
- **Team: 6 universities, one industry partner, ~30 faculty**

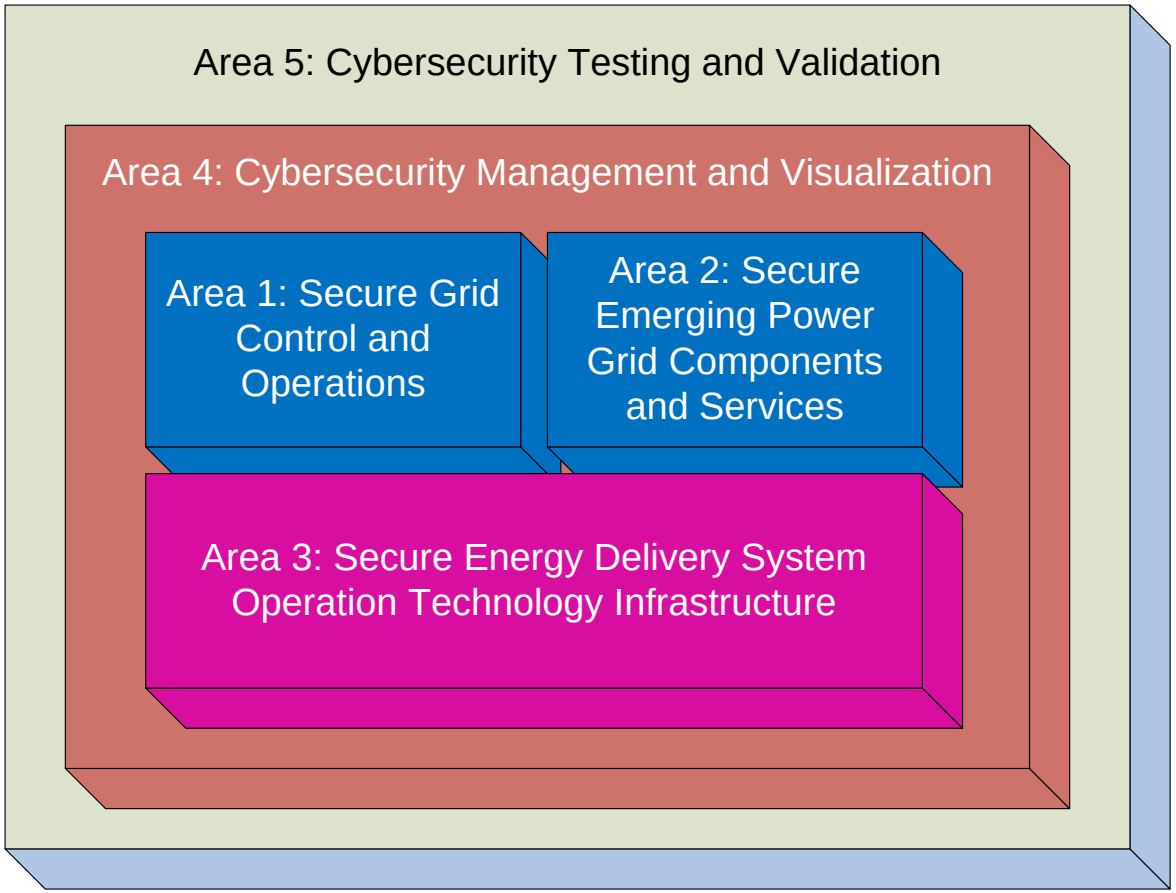
Performer:	**University of Arkansas**
Partners:	**Arkansas Electric Cooperative Corporation** **Carnegie Mellon University** **Florida International University** **Lehigh University** **Massachusetts Institute of Technology** **University of Arkansas, Little Rock**
Federal Cost:	**$12.2M**
Cost Share:	**$3.1M**
Total Value of Award:	**$15.3M**

Plans to transfer technology/knowledge to end user

- Targeted end user for the technology: facility owners and vendors
  - Facility owners: cybersecurity management and visualization tools, situational awareness tools, vulnerability/patch management tools
  - Vendors: customized intrusion detection technologies, data forgery detection tools, security data analytics tools
- Plans to gain industry acceptance (industry-driven approach for research)
  - Security needs take input from industry
  - Project selection suggested by industry
  - Technology design takes feedback via industry focus group activities
  - Beta testing of technologies conducted at industry partner AECC
  - Communications to industry through avenues in addition to academic publications

Research Activity Areas

Research Areas



Sample Research Projects

Cybersecurity for Energy Delivery Systems

- **Data Integrity Attacks**
  - Power state estimation, automatic generation control, topology attacks
- **Time synchronization attacks**
  - PMU
- **Intrusion detection**
  - Compromised device detection
  - Quickest intrusion detection
- **Communication security**
  - Botnet and Intrusion Detection in SCADA Networks
  - Secure Time-Critical Communications in Substations
  - Secure Smart Metering Communications
- **Power electronics security**

What DOE Cares

- **Address real and important security problems**
  - **University-industry collaboration highly encouraged**
- **Security technologies should be integratable to the existing infrastructure**
- **Security technologies should survive (or evolve with) the evolvement of security threats**
- **Technology transfer to the energy sector**

Thank you!