

# Consolidated Innovative Nuclear Research (CINR) Fiscal Year (FY) 22 FOA Webinar

## CT-1: NEET/CTD Cybersecurity R&D

Rebecca Onuschak  
Office of Nuclear Energy  
Department of Energy

August 12, 2021

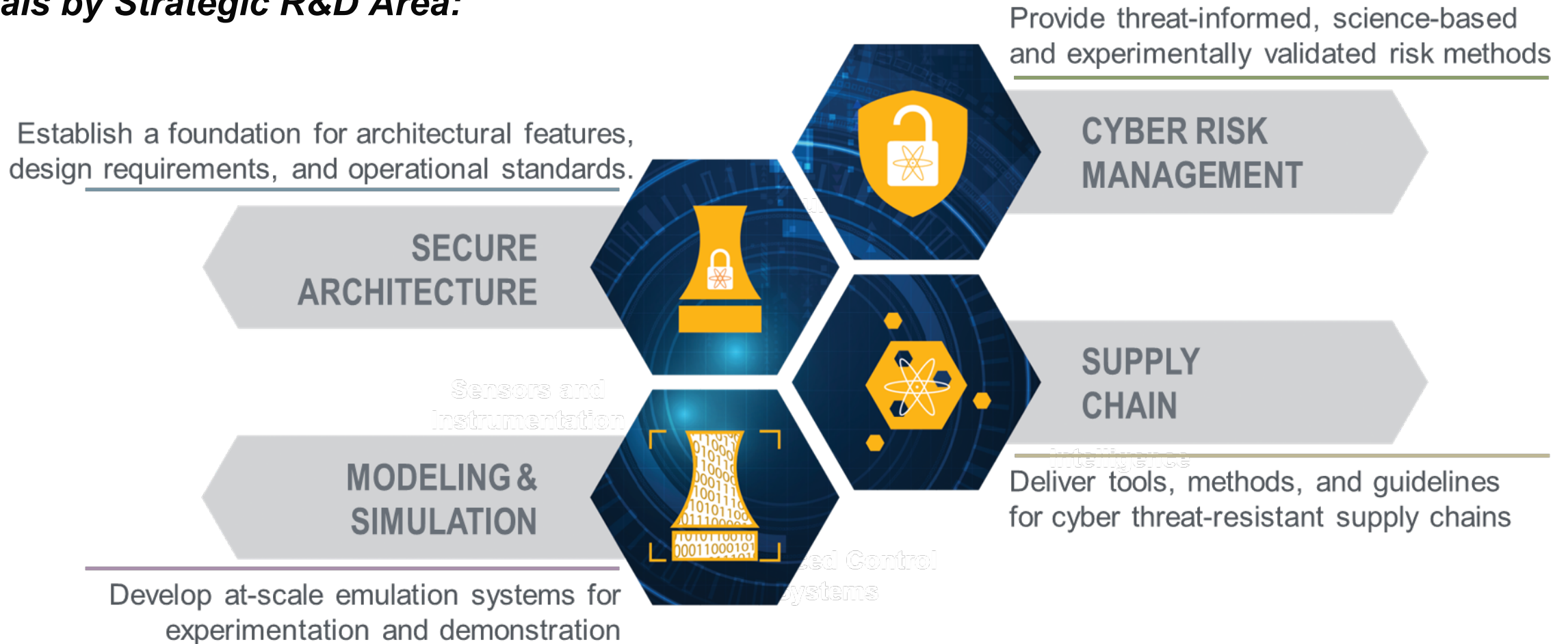
Federal POC – Rebecca Onuschak  
[rebecca.onuschak@nuclear.energy.gov](mailto:rebecca.onuschak@nuclear.energy.gov)

Technical POC: Lon Dawson  
[ladawso@sandia.gov](mailto:ladawso@sandia.gov)

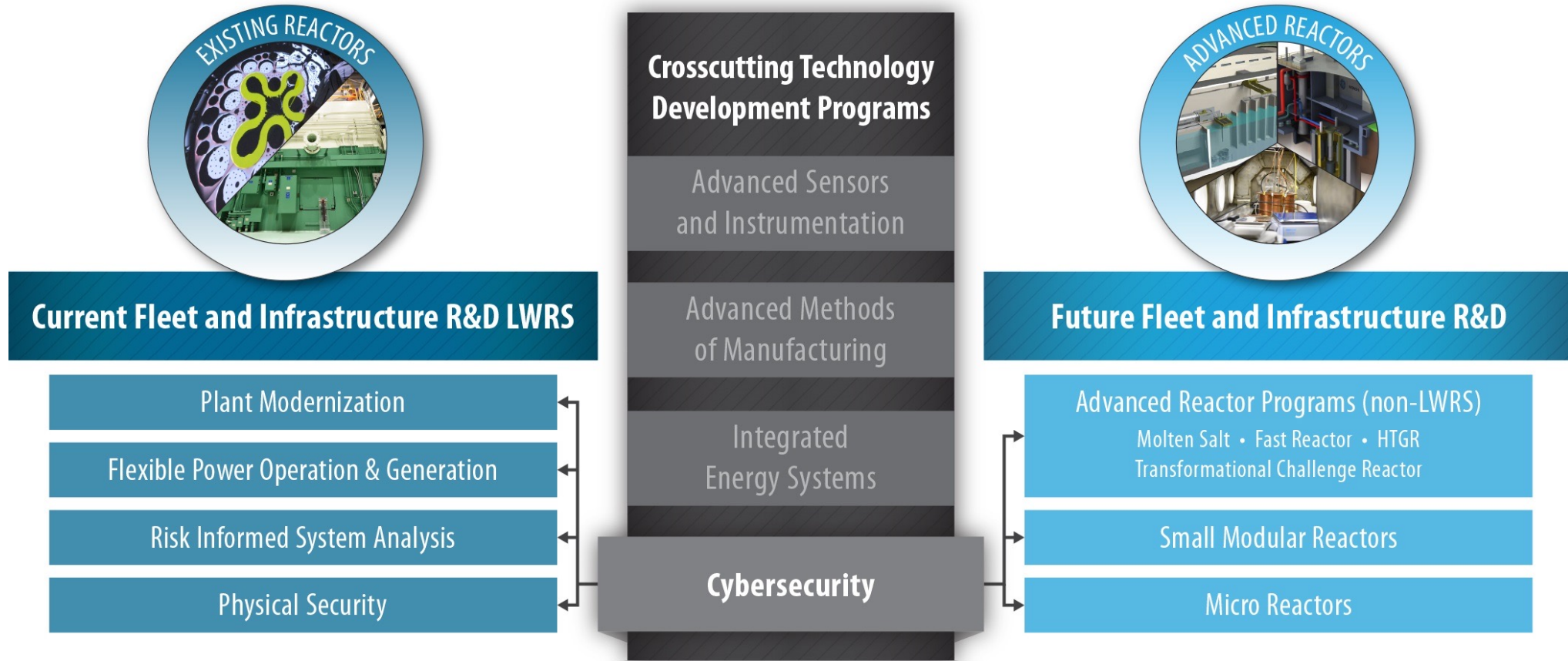
# Cybersecurity R&D Program Overview

**Mission:** Enable science-based methods and technologies for cost-effective, cyber-secure digital instrumentation, control and communication for current and future nuclear power plants.

**Goals by Strategic R&D Area:**



# Connections to other R&D programs, NRC, Industry



**Stakeholders, Peers, Partners**  
(Industry, Industry Associations, Universities, Regulators)



# 2021 NEUP Call Interests

- The DOE-NE Cyber Security program seeks to perform R&D in technologies that support and enable digital solutions for the U.S. nuclear sector.
- Proposals are sought for research and development to enable secure communication for future reactor technologies, specific to safety- and security-related sensors and/or controls. Areas of interest include cybersecurity research that enables advanced reactor control concepts including the potential for remote reactor operations.
- Compelling proposals should include aspects of:
  - Secure communications for control and monitoring systems to enable remote operations;
  - Secure communications to support expanded use of data for operational decision making.
- Topics not of interest include:
  - General-purpose attack scenario models or intrusion detection tools for plant operations.
  - Development of technologies, tools or methods generally applicable to industrial control systems, except to adapt these for use in the regulatory and operational context of nuclear power plants.



# Previously Awarded Cybersecurity NEUP Areas

## Nuclear Cyber NEUP – R&D Focus Areas

### **Cyber Risk Management:**

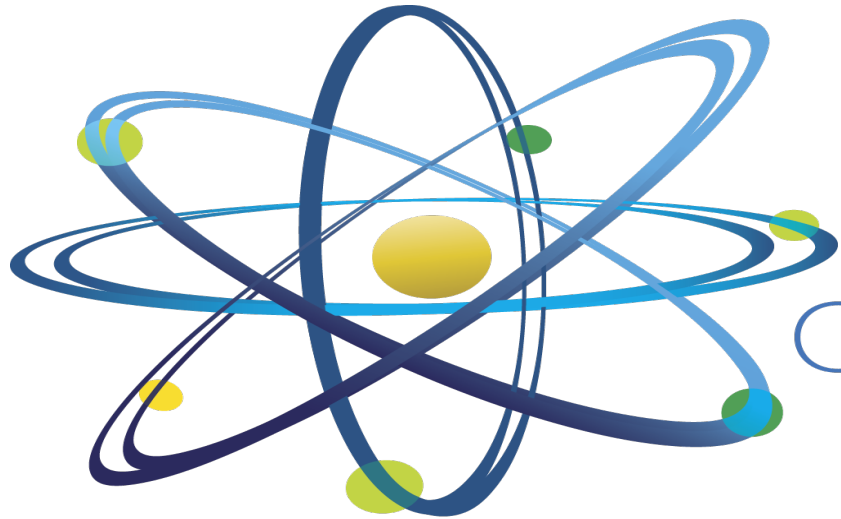
- *Methodology Development for Cybersecurity Robustness and Vulnerability Assessment of University Research Reactors: A Case Study Using the PULSTAR Reactor*
- *Cyber Security Analysis for Nuclear Reactor Control Systems*
- *Support for Reactor Operators in Case of Cyber-Security Threats*

### **Modeling and Simulation:**

- *NICSim: Nuclear Instrumentation and Control Simulation for Evaluating Response to Cyber-attacks*
- *Model-Based Diagnostics and Mitigation of Cyber Threats*
- *Development of Information Trustworthiness and Integrity Algorithms for Cybersecurity Defenses of Nuclear Power Reactors*

### **Secure Architecture:**

- *CyberSim: A Flexible Simulation Environment for the Evaluation of Cyber Risk in Nuclear Power Plants in Support of the Design of Cyber Protection Architectures*
- *A Cyber-Attack Detection Platform for Cyber Security of Digital Instrumentation and Control Systems*
- *Un-hackable Communications with Quantum Key Distribution for Secure Remote Operations*



Clean. **Reliable. Nuclear.**