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:

- **Secure Architecture**: Establish a foundation for architectural features, design requirements, and operational standards.
- **Cyber Risk Management**: Provide threat-informed, science-based and experimentally validated risk methods.
- **Supply Chain**: Deliver tools, methods, and guidelines for cyber threat-resistant supply chains.
- **Modeling & Simulation**: Develop at-scale emulation systems for experimentation and demonstration.
Connections to other R&D programs, NRC, Industry

Current Fleet and Infrastructure R&D LWRS
- Plant Modernization
- Flexible Power Operation & Generation
- Risk Informed System Analysis
- Physical Security

Crosscutting Technology Development Programs
- Advanced Sensors and Instrumentation
- Advanced Methods of Manufacturing
- Integrated Energy Systems
- Cybersecurity

Future Fleet and Infrastructure R&D
- Advanced Reactor Programs (non-LWRS)
  - Molten Salt • Fast Reactor • HTGR
  - Transformational Challenge Reactor
- Small Modular Reactors
- Micro Reactors

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

CT-1: 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