U.S. DEPARTMENT OF ENERGY | Nuclear Energy

Cyber Security R&D (NE-1)

Trevor Cook

Office of Nuclear Energy
U.S. Department of Energy

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

NE Cyber Security R&D

Objectives:

- **To strength security through reduction of vulnerabilities**
- **To mitigate the consequences of threats**
- **To lower the costs of protection and compliance**
- **To provide a collaborative pathway for industry and researchers**

Fields of Interest:

- **Risk Management – Secure Architectures and Supply Chain**
- **Modeling & Simulation**
- **Information Sharing/Training/Education**

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

NEUP Proposal Interest - R&D Needs

- **Research of most interest will addresses characteristics and behaviors of components within embedded instrumentation and control (I&C) systems that are used within the nuclear enterprise.**
- **Modeling and Simulation shall capture the behavior of an I&C system, to**
  - 1) simulate characteristics of an I&C system under cyber attack;
  - 2) study the cyber risk impacts of upgrades and maintenance on such systems;
  - 3) enable future nuclear energy cyber security research, and
  - 4) facilitate nuclear facility operation education and training.
- **Secure Architecture Attributes**
  - Resistant to common cause failures/vulnerabilities
  - Resilient to cyber attacks and able to detect intrusions
  - Economical to manufacture, install, and maintain

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Contact Information

- **For NEUP, interested parties may contact the INL cyber security program manager at steven.hartenstein@inl.gov**
- **Interested parties may contact me as well at trevor.cook@nuclear.energy.gov**