Digital command and control environments demand an integrated approach to nuclear cybersecurity. INL works with the nuclear community to understand cyber and physical security risks to develop successful mitigation strategies.

Integration of Nuclear Cyber and Physical Security

INL meets the unique cybersecurity requirements of the network and operational environment

Instrumentation and control (I&C) within nuclear facilities are continuously connected with information technology and wireless communications in facilities and operations to address efficiencies, cost savings and convenience. In this digital command and control environment, the use of physical boundaries alone is inadequate to secure nuclear technology and facilities. An integrated cyber physical security approach is essential to address the resiliency of the facility and continuity of operations.

Idaho National Laboratory employs the foremost cyber and industrial control systems security experts in the world. The lab works with the international nuclear community to assist them in understanding cyber and physical security risks and to develop mitigation strategies and techniques to meet the

Continued next page

The Energy of Innovation

Idaho National Laboratory

Continued from previous page

unique requirements of network and operational environments.

Cybersecurity assistance is provided by understanding the capabilities of malicious actors and developing customized mitigation technologies and tactics to meet the configuration requirements of installations at nuclear facilities and the protection of radioactive materials in and out of regulatory control. This enables the nuclear industry to address a sustainable long-term approach to nuclear cybersecurity that increases the security posture and manages the evolving and emerging threats of nuclear proliferation and terrorism.

INL's unique capabilities in nuclear and cybersecurity include:

- Internationally recognized nonproliferation experts with real-world experience and backgrounds in nuclear facility inspection, physical protection, modeling and simulation, material science, physics and engineering.
- Comprehensive instrumentation and control, cyber and nuclear nonproliferation capabilities with similar nuclear infrastructure and examination equipment found worldwide.
- Inclusive nuclear security approach that allows for field and laboratory technology evaluation.
- Replication of typical control system network for architecture reviews and system hygiene to support asset owners in securing their systems.
- Protocol analysis, reverse engineering and forensics to advance persistent threat mitigations for the nuclear industry.
- Cyber-informed risk methods and unique engineering designed tools and methodologies to anticipate cyber and physical security risk and investment strategies.
- Frameworks for prioritization of investments and threat indicators for high-consequence activities.

INL is an internationally recognized thought leader on industrial control systems cybersecurity across multiple domains: vulnerability assessments, mitigation research and development, future architectures, policies and processes.

INL has proven that intelligent sensors and wireless communications can be integrated effectively with embedded security; secure industrial control systems can reduce the threat of cyberattack; and that physical devices and barriers are part of the overall security posture.

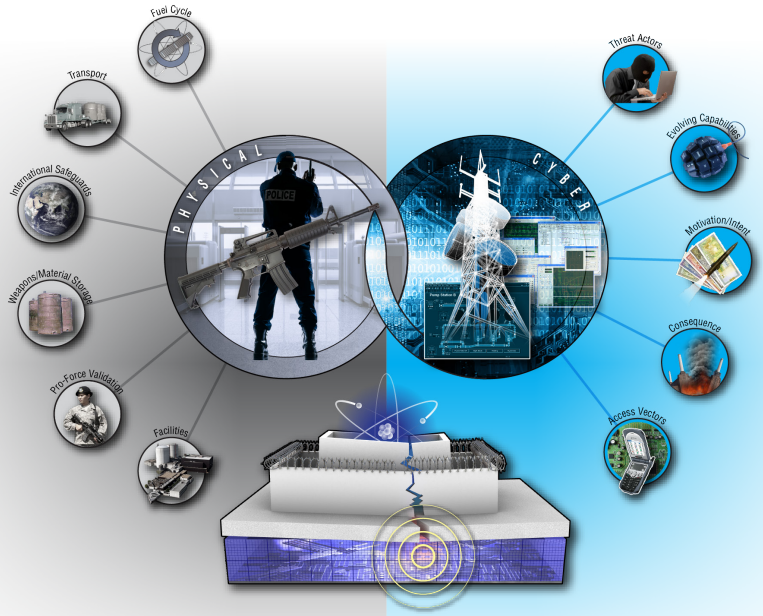
INL's nuclear security programs are fundamentally changing how the nation and world approach analysis of threats to the complex myriad cyber-physical systems.

For more information

Misty Benjamin
(208) 526-5940
misty.benjamin@inl.gov

nuclearcyber@inl.gov
www.inl.gov

A U.S. Department of Energy National Laboratory



Vulnerabilities in digital system potentially compromise physical security.

15-GA50086 05-15