INL researchers inspect circuit boards, electronic components and chip sets as part of the lab's control systems cybersecurity mission.

Cybersecurity Capabilities

Idaho National Laboratory (INL) is a world leader in securing critical infrastructure systems and improving the resiliency of vital national security and defense assets. The laboratory has significant capabilities and expertise to confront and overcome the growing challenges posed by increasingly adept and malicious cyber actors, as well as disruptive events from weather-related disasters or geomagnetic phenomenon.

SECURING INDUSTRIAL CONTROL SYSTEMS

INL researchers work to secure industrial control systems and digital automation devices commonly found at power and renewable energy utilities, oil and natural gas refineries, water treatment plants, and manufacturing facilities. These systems and devices include:

- energy management systems,
- process control systems,
- programmable logic controllers, and
- supervisory control and data acquisition systems.

Led by the Cybercore Integration Center, INL brings together multidisciplinary teams of seasoned control systems cybersecurity analysts, experienced power engineers, cyber researchers, and control systems experts to perform cutting-edge analysis, incident response, training, and tool and technology development.

The laboratory's cybersecurity experts represent a unique fusion of academic training and professional expertise. They combine traditional all-source threat analysis with the technical acumen associated with engineering and systems documentation, operational technology networks, programming languages, and foreign language skills to produce sound analytic products. They have demonstrated proficiency in analytic standards and tradecraft and maintain a strategic perspective of the security landscape to analyze evolving cyberthreats targeting the operational technology environment. By maintaining a deep awareness of newly discovered vulnerabilities within industrial control systems, the lab's experts understand adversarial cyber capabilities and the subsequent consequences posed to critical infrastructure.

INL
Idaho National Laboratory

INL also supports and administers large-scale programs for the U.S. Department of Energy, National Nuclear Security Administration, and the Department of Defense. Some programs include INL's signature Consequence-driven Cyber-informed Engineering (CCE) methodology, the Cyber Testing for Resilience of Industrial Control Systems (CyTRICS) program, the Cyber Analytics Tools and Techniques (CATT) program and the Cybersecurity for the Operational Technology Environment (CyOTE) program.

IMPROVING INFRASTRUCTURE RESILIENCY

In addition to pioneering work in industrial control systems cybersecurity, INL has signature capabilities in infrastructure resiliency, geographical information systems, data visualization, and advanced instrumentation and controls. Led by the INL Resilience Optimization Center, the laboratory draws on its deep expertise, resources and abilities to support government, academic and private industry organizations to understand and account for the interdependencies and interoperabilities of critical assets.

INL's resiliency research and testing is focused on designing and developing infrastructure components, systems, and programs where monitoring, control and human interaction must seamlessly integrate. The laboratory has a range of research facilities and test beds dedicated to sensors, controls and intelligent systems research. These facilities can be utilized for complex evaluation of control system designs for cybersecurity, advanced control or operational verification and validation. As a leading provider of research, testing and training services to the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the laboratory also supports key homeland security activities aimed at protecting and safeguarding critical assets and capabilities.

For more than a decade, INL experts have supported DHS' Regional Resiliency Assessment Program designed to help private sector infrastructure owners and operators, emergency response and recovery organizations, and utility providers to assess and identify potential vulnerabilities in their systems and address them before consequences arise. Through this program, INL experts work with state and local government officials analyzing high consequence systems ranging from dams to fault lines to supply chain infrastructure. The team also provides critical product evaluations that analyze consequential systems and processes for cyber vulnerabilities and resiliency improvements. These evaluations have been instrumental in improving U.S. election system technology, as well as analyzing foreign malware and exploit code that could impact U.S. critical infrastructure.

QUICK FACTS

- INL has more than 150,000 square feet of laboratory space dedicated to industrial control systems cybersecurity, grid and wireless security, and infrastructure resiliency.
- The laboratory's 890-square-mile desert Site includes multiple test ranges, including a power grid test bed, water security test bed, and wireless test bed.
- Our Critical Infrastructure Test Range Complex can perform bench-scale to full-scale testing of equipment and new technology from concept to destructive analysis.
- INL employs hundreds of experts with backgrounds and capabilities in cybersecurity, power systems, engineering, system resilience, vulnerability assessments and threat analysis.
- The laboratory is a key contributor, facilitator and advocate for cybersecurity and infrastructure resiliency education and workforce development, providing training to thousands of individuals and students each year.

FOR MORE INFORMATION

Technical Contact

Dr. Char Sample
Chief Cybersecurity Research Scientist
(208) 526-4212
Charmaine.Sample@inl.gov

General Contact

Ethan Huffman
Marketing and Engagement
(208) 526-5015
ethan.huffman@inl.gov

www.inl.gov

A U.S. Department of Energy National Laboratory

20-50444-001-R0