Homeland Security Enterprise Support Overview

Idaho National Laboratory

Laboratory Background

Idaho National Laboratory (INL) is one of the U.S. Department of Energy's (DOE) national laboratories and is managed by Battelle Energy Alliance (BEA) for DOE's Office of Nuclear Energy. Located in Idaho Falls, ID, INL employs more than 5,740 researchers and support staff focused on innovations in nuclear research, renewable energy systems, and security solutions that are changing the world. Since its inception in 1949, INL has created products and developed solutions that are saving lives from the home front to the battlefield.

Mission

INL's national security missions focus on protecting the nation's critical infrastructures and preventing the proliferation of weapons of mass destruction. Within both areas, INL leverages its scientific expertise, applied engineering discipline, build-test-build problem-solving approach, and unique infrastructure to develop military, homeland security, energy, and industry solutions.

Expertise

The INL Resilience Optimization Center (IROC) leverages laboratory-wide capabilities and expertise to deliver unique systems resilience and risk management solutions for our programs and partners. Specific capabilities include Systems Engineering, Clean Energy & Transportation, Power & Energy Systems, Modeling and Simulation, Artificial Intelligence and Machine Learning, Risk Assessment, Workforce Development, Human Factors, Control Systems Cybersecurity, Electric Grid Resilience, Vulnerability Analysis, Wireless Communications, Radio Frequency Modeling, Emergency Training and Response, Cybersecurity Training, and Armor Development.

INL's National and Homeland Security Testing Facilities are singularly positioned to support a wide variety of research, analysis, testing and validation opportunities for defense, federal, and industrial collaborators. INL's 890 square-mile footprint makes it the largest lab geographically. Comprised of a cyber-physical infrastructure test range, co-located laboratories, several dedicated test ranges, and available airspace, this premier research park allows testing – from modeling and simulation to full-scale – to be conducted safely and securely.

Unique facilities and laboratory infrastructure related to the Homeland Security Enterprise (HSE) mission:

- Biomass Feedstock National User Facility
- Controls Environment Laboratory Resource
- Critical Infrastructure Test Range Complex
- Cybercore Integration Center
- Cybersecurity Analysis Center
- Electric Vehicle Test Laboratories
- Energy Systems Laboratory
- Explosive Test Range
- Nuclear Materials Laboratory
- Radiological Response Training Range
- Specific Manufacturing Facility
- Unmanned Aerial Vehicle Test Bed
- Vulnerability & Verification Laboratory
- Wireless R&D Laboratories
- Wireless Test Range
- Water Security Test Bed

Capability highlights at these testing facilities include:

- Several firing ranges and a blast ceiling of 20,000 pounds
- Over 60 miles of 138kV, multiple substations and power grids
- Cellular, microwave, satellite, and fiber-optic backhaul wireless communication systems
- Over 100,000 square feet of cybersecurity labs, collaborative spaces, and secure meeting spaces
- Municipal water system with pressurized pipelines, household systems, and automated controls
- Over 3,000 square miles of Federal Aviation Administration (FAA) Certificate of Authorization (COA) airspace with a 1,000-foot unmanned aerial systems runway

Major Customers in the Homeland Security Enterprise

- Department of Homeland Security
  - Countering Weapons of Mass Destruction
  - Cybersecurity & Infrastructure Security Agency
  - Immigrations and Customs Enforcement
  - Federal Emergency Management Agency
  - Office of the Chief Readiness Support Officer
  - Office of Operations Coordination
  - Science & Technology Directorate
  - Transportation Security Administration
- Department of Transportation
  - Federal Aviation Administration
- Department of Energy
- Department of Defense
- International, State and Local Governments
- Private Industry
- Universities and Colleges

Impact Snapshots

All Hazards Analysis (AHA) Framework: A dynamic analytical framework that utilizes data about critical infrastructure to enable knowledge discovery and decision support. AHA can simulate possible scenarios that might impact critical infrastructure, from natural disasters to addition of new equipment. It can identify interdependencies within the infrastructure systems and help decision-makers to understand how and where the systems interrelate.

Commercial Routing Assistance (CRA): The CRA Tool is an interactive website that maps routes and displays information about state government actions that can impact interstate transportation. It can provide routes for commercial, emergency, and disaster response vehicles to travel into or around various states in an efficient, compliant, and safe manner. This tool supports the efficient and effective operation of the trucking industry, helping to ensure the delivery of goods and resources to government, industry, and the American public.

Consequence-Driven Cyber-Informed Engineering (CCE): CCE is a methodology focused on securing the nation's critical infrastructure systems. CCE begins with the assumption that if a critical infrastructure system is targeted by a skilled and determined adversary, the targeted network can and will be penetrated. This 'think like the adversary' approach provides critical infrastructure owners and operators with a four-step process for safeguarding their critical operations.

Constrained Cyber Communication Device (C3D): With the main goal of detecting and blocking grid cyberattacks, C3D uses advanced communication capabilities to autonomously review and filter commands being sent to protective relay devices. The C3D device sits deep inside a utility's network, monitoring and blocking cyberattacks before they impact relay operations.

Cyber Competency Health and Maturity Progression (Cyber-CHAMP) Framework : Cyber-CHAMP Framework is a customizable workforce solution for public and private sector entities to understand their cybersecurity operational readiness in relation to established objectives and provides a roadmap on how to achieve these goals. It helps users discover their cybersecurity knowledge and skill gaps, by individual or organization, resulting in a direct Return on Investment (ROI).

OmniTap: OmniTap provides universal capture and translation of both modern and legacy industrial control systems communication, enabling cybersecurity sensors to be deployed within any ICS environment. A tool that can translate existing proprietary ICS communication, OmniTap will enable current IT cybersecurity tools to be used on ICS networks today.

OpDefender: OpDefender, an intelligent software-defined networking switch, protects electric utilities, oil and gas infrastructure, water systems, and other critical infrastructure from cyberattack. OpDefender integrates physical and software components into a small device that can either replace or work in concert with existing network switches.

Plug-N-Play Appliance for Resilient Response of Operational Technologies (PARROT): PARROT provides an extra layer of security from cyberattacks on critical infrastructure operations by placing it between control systems and infrastructure. It isolates cyberattacks, provides a manual or automated response, and prevents harmful impacts while maintaining operations.

Route Operable Unmanned Navigation of Drones (ROUNDS): ROUNDS is a cost-effective method for drones to self-navigate a course inside a building or structure where a strong GPS signal is absent. ROUNDS helps a wide range of industries save time, reduce cost, and increase efficiency while reducing human exposure to heights, chemicals, radiation, and other hazards.

Storm Damage Estimate Prediction and Recovery Tool (Storm-DEPART): Storm-DEPART combines critical infrastructure inventory data with weather forecasts to predict weather-related damages to an electricity utility service provider's assets. It also estimates recovery support that will be needed to restore normal operations, including time, materials, and resources.

Wireless radio Frequency signal Identification and protocol Reverse Engineering (WiFIRE): WiFIRE is a hardware-software appliance that can rapidly identify authorized/unauthorized wireless communications activity in a facility or geographic area and provides a single toolset for monitoring the wireless spectrum.