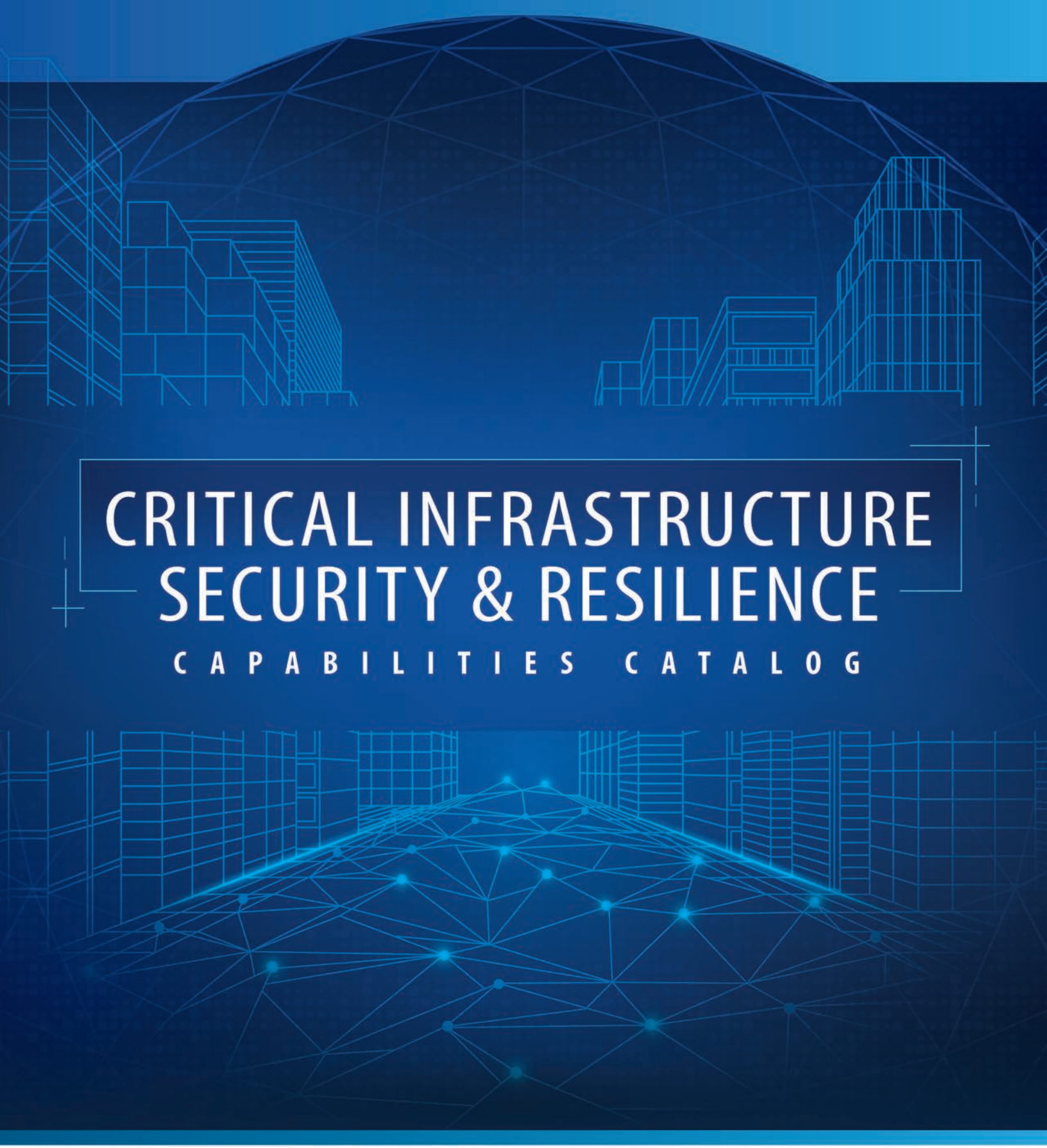


CRITICAL INFRASTRUCTURE SECURITY & RESILIENCE

CAPABILITIES CATALOG

Idaho National Laboratory

OVERVIEW

The systems that power homes, deliver clean water, move goods and fuel the economy are under growing threat. Adversaries are probing control systems. Extreme weather is stressing aging infrastructure. Supply chains carry hidden risks. And the consequences of failure, measured in lives, economic instability and national security, have never been higher.

The Idaho National Laboratory's critical infrastructure security and resilience capabilities are designed to address these challenges. INL integrates its engineering, cybersecurity, data science and policy expertise to protect and strengthen the systems on which the nation relies, ensuring critical functions persist even when defenses are compromised.

VISION

Our vision is to ensure the nation's critical infrastructure continues to operate through compromise.

MISSION

Our mission is to enable the development, operations and maintenance of resilient critical infrastructure systems, focusing on people, processes and technology.

SECURING THE NATION'S CRITICAL INFRASTRUCTURE

Sectors Served

INL's Critical Infrastructure Security and Resilience (CISR) capabilities protect and strengthen infrastructure across all 16 critical infrastructure sectors, with specialized depth in:

- **Electric power grid:** generation, transmission and distribution
- **Oil and natural gas:** pipelines, processing and control systems
- **Water and wastewater:** treatment, distribution and automated controls
- **Communications:** fiber, wireless and satellite networks
- **Transportation:** including aviation, port operations, mass transit and more
- **Nuclear energy:** integrated energy systems and microreactor applications
- **Defense industrial base:** mission-critical infrastructure and continuity



INL CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE CORE CAPABILITIES:

1. Infrastructure security
2. Infrastructure modeling, simulation and tool development
3. Infrastructure resilience analysis
4. Energy systems supply chain analysis
5. Super intelligence/machine learning security and assurance
6. Infrastructure hardening and resilient design
7. Stakeholder preparedness and technical assistance

MORE INFO

1 INFRASTRUCTURE SECURITY

INL's Critical Infrastructure Test Range Complex provides a full-scale environment to research, develop and validate technologies that strengthen U.S. infrastructure security and resilience. Leveraging real-world grid systems, fiber-optic and wireless communications, water security facilities, and flexible test pads, CITRC enables end-to-end testing of energy, communications and lifeline-sector technologies under true operating conditions.

CAPABILITIES INCLUDE:

- Infrastructure security analysis across lifeline sectors
- Applied concept-to-commercialization engineering
- Full-scale research through development, demonstration and deployment for energy infrastructure operations and testing
- Grid-enhancing technologies and power grid transformation
- Signal phenomenology to test advanced mitigation devices that can help protect critical infrastructure from electromagnetic events
- Vendor-specific OT expertise across energy, water and industrial control environments
- Integrate power sources, including nuclear power technology systems, for resilient energy generation
- Pipeline and industrial control system security for oil and natural gas operations



MORE INFO

Electric Grid Security

AT-SCALE INFRASTRUCTURE TESTING

INL's 890-square-mile site hosts onsite test beds enabling full-scale, real-world evaluation of critical infrastructure systems across multiple sectors — not just in simulation, but under real operational conditions.

Electric Power Grid Test Bed

INL's full-scale electric power system test bed evaluates grid behavior, security, reliability, and resilience. Using configurable transmission and distribution environments, stakeholders can validate technologies, identify vulnerabilities, and evaluate system response across a range of scenarios.

Features of test bed:

- Expert engineers and researchers skilled in innovative test setups and advanced industry applications
- Grid technologies tested in real-world conditions including freezing winters, high-temperature summers and wildfire hazard conditions
- Transmission and distribution substations built to industry standards
- 16 miles of transmission lines (up to 345 kilovolts)
- 5 miles of overhead distribution lines (up to 35 kV)
- Substations linked by fiber-optic 2G–5G wireless networks
- Realistic grid-edge controllers and devices complemented by cybersecurity simulations
- Fault initiation and megawatt power delivery with an on-site line crew



MULTI-SECTOR TESTBED OPPORTUNITIES

Includes:

- Microreactor grid integration and resilience testing
- Oil and natural gas pipeline monitoring and control system evaluation
- Transportation and port logistics simulation
- Energy Technology Proving Ground

Water Security Test Bed

Testing for water and wastewater system security using pressurized pipelines, household systems, and automated control interfaces to evaluate cyber-physical vulnerabilities and resilience strategies

Wireless and Communications Test Bed

Features 2G–5G cellular, high frequency, microwave, satellite, and fiber-optic backhaul for evaluating communications infrastructure and grid edge connectivity

Unmanned Aerial Systems (UAS) Test Range

Over 8,000 square miles of FAA-authorized airspace with a 1,000-ft UAS runway, supporting infrastructure inspection, wildfire response and fault assessment applications

CURRENT RELATED PROJECTS:

WILD GRID

Reducing wildlife-related outages

Novel resonance seismic resiliency

Improving seismic resilience of large power transformers

Mechanical solutions for grid protection

Extending grid component life

Wildfire fault testing

UAS drop tests, fault initiation, and fire department response

Power phenomenology

Minimizing effects of geomagnetic disturbances

MORE INFO

WILD GRID

Novel resonance seismic resiliency

Mechanical solutions for grid protection

Wildfire fault testing

2 INFRASTRUCTURE MODELING, SIMULATION AND TOOL DEVELOPMENT

INL develops advanced modeling, simulation, digital engineering, and decision-support tools that help stakeholders understand, predict, and improve how critical infrastructure systems perform and withstand disruptions. Combining engineering analysis with operational data, geospatial information, and knowledge of how different infrastructure systems depend on one another allows INL to deliver actionable insights that support planning, preparedness, risk management, technology evaluation, and operational decision-making across sectors.

CORE CAPABILITIES

- Infrastructure modeling and simulation of cyber-physical systems, industrial control systems and critical infrastructure networks
- Cross-sector dependency analysis to identify vulnerabilities, cascading impacts and resilience opportunities
- Mission planning, consequence forecasting, and scenario-based analysis supporting preparedness, continuity and emergency response
- Developing custom decision-support tools, dashboards, predictive analytics platforms and software applications
- Cyber risk assessment, supply chain analysis and infrastructure security decision support



REPRESENTATIVE TOOLS AND PLATFORMS

FORECASTING AND PLANNING:

Acclimate

Long-term climate and extremeweather risk planning for utilities and infrastructure operators

Storm-DEPART (Damage Estimate Prediction and Recovery Tool)

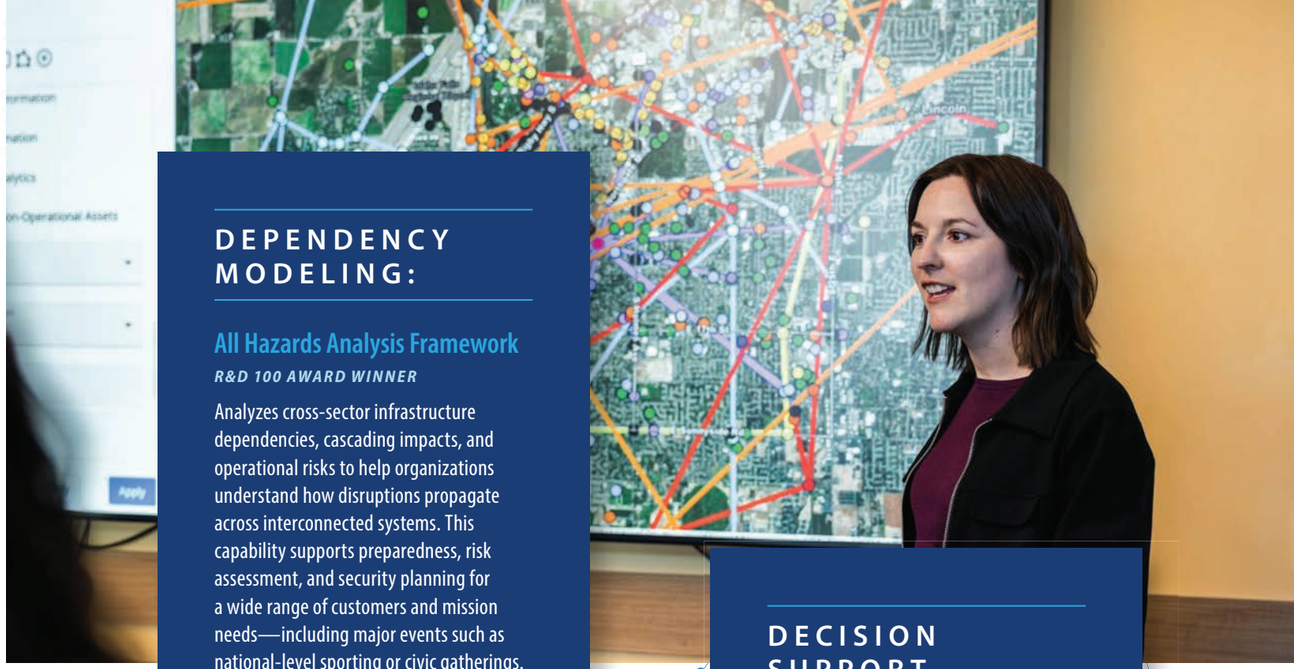
R&D 100 AWARD WINNER

Storm damage prediction and recovery forecasting for electric infrastructure

MORE INFO

Acclimate

Storm - DEPART



DEPENDENCY MODELING:

All Hazards Analysis Framework

R&D 100 AWARD WINNER

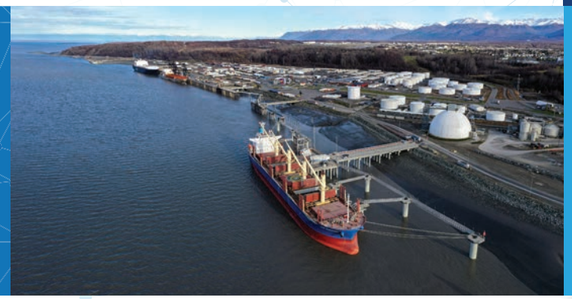
Analyzes cross-sector infrastructure dependencies, cascading impacts, and operational risks to help organizations understand how disruptions propagate across interconnected systems. This capability supports preparedness, risk assessment, and security planning for a wide range of customers and mission needs—including major events such as national-level sporting or civic gatherings.

Infrastructure Dependency Wheel

Visualization of cross-sector infrastructure interdependencies

MORE INFO

All Hazards Analysis Framework



DECISION SUPPORT SYSTEMS:

Maritime Domain Awareness Tool

Maritime and port resilience decision-support tool for emergency response and recovery

Statewide Cyber Dashboard

A state-level capability that evaluates, improves, and visualizes cybersecurity risk across infrastructure, supported by a centralized dashboard that turns assessment data into actionable sector, geographic, and system-level insights

MORE INFO

Maritime Domain Awareness Tool

3 INFRASTRUCTURE RESILIENCE ANALYSIS

INL delivers integrated cyber-physical infrastructure analysis that enables stakeholders to strengthen security, resilience, and mission preparedness. By applying interdisciplinary analytical approaches and risk-management tools, the laboratory supports improvements across all lifeline sectors.

CORE CAPABILITIES:

Multisector infrastructure analysis

INL conducts comprehensive infrastructure assessments that evaluate interdependencies, vulnerabilities and operational risks across multiple critical infrastructure sectors. Analyses are tailored to sponsor missions and may support strategic planning, operational preparedness or resilience investment decisions.

Emergency management and continuity planning

Emergency management organizations and infrastructure operators are supported through mission-focused preparedness and continuity analysis that helps them understand operational dependencies, identify mission-critical functions, and evaluate resilience strategies before, during, and after disruptive events.

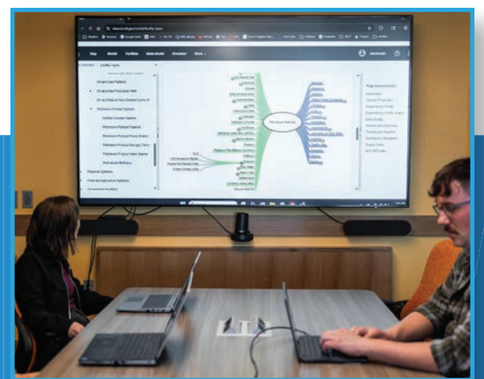
Geospatial science and visualization

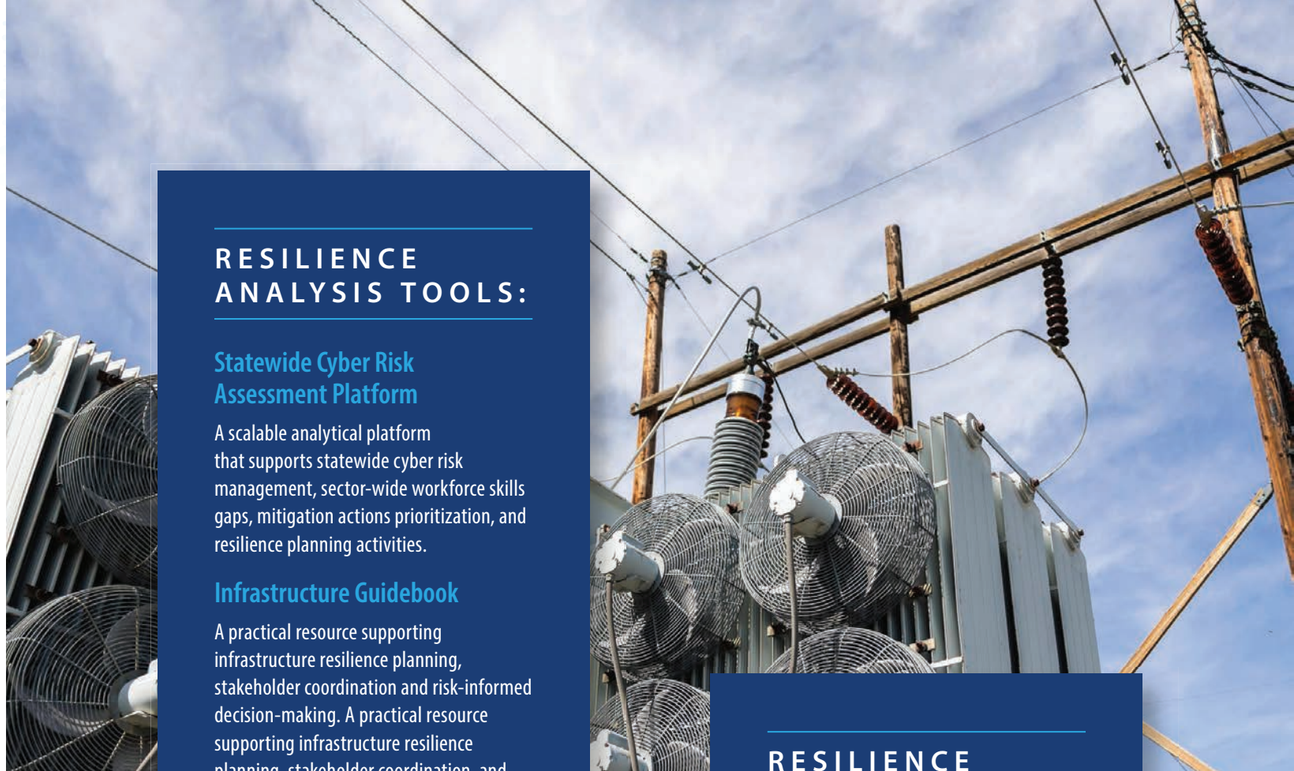
Analysts apply advanced geospatial science, remote sensing, and visualization technologies to collect, integrate, and analyze infrastructure data. These capabilities support operational awareness, planning, incident response and stakeholder decision-making.

Intelligence-informed infrastructure analysis

INL integrates open-source and restricted-source information with infrastructure expertise to identify vulnerabilities, assess emerging threats, and support sponsor planning and operational decision-making.







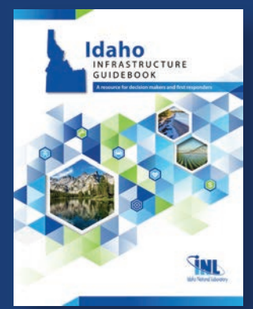
RESILIENCE ANALYSIS TOOLS:

Statewide Cyber Risk Assessment Platform

A scalable analytical platform that supports statewide cyber risk management, sector-wide workforce skills gaps, mitigation actions prioritization, and resilience planning activities.

Infrastructure Guidebook

A practical resource supporting infrastructure resilience planning, stakeholder coordination and risk-informed decision-making. A practical resource supporting infrastructure resilience planning, stakeholder coordination, and risk-informed decision-making.



MORE INFO

CSET: Cyber Security Evaluation Tool

Idaho Infrastructure Guidebook

RESILIENCE ANALYSIS TOOLS *(CONTINUED)*:

Regional Resilience Guide

A resilience planning methodology and implementation resource supporting regional infrastructure preparedness and recovery planning. Regional Resilience Guide: A resilience planning methodology and implementation resource supporting regional infrastructure preparedness and recovery planning.

MORE INFO

Regional Resilience Guide

4 ENERGY SYSTEMS SUPPLY CHAIN ANALYSIS

INL leads in analyzing organizational, component, and digital supply chains affecting the resilience of energy, water, oil and natural gas, defense, and other critical infrastructure sectors. Through advanced, data-driven methods, researchers uncover vulnerabilities, map hidden supply chain relationships, and provide insights enabling risk-informed decisions.

By examining organizational and business linkages, INL identifies adversarial influence and cyber supply-chain risks threatening multiple sectors. INL boosts national supply chain resilience through providing procurement decision support tools, rapid cyber-risk assessments, and systems-of-systems. modeling that reveals the potential for supply or cyber risk.





SUPPLY CHAIN CAPABILITIES:

Supply chain analysis

Analyze critical supply chains across key energy-sector systems to identify essential vendors, components, and the potential risks these pose to asset owners.INL's supply chain analysis reports support industry and government partners by providing insights that help them design effective supply chain risk-mitigation strategies

Procurement tool

Helps users navigate procurement guides via a decision tree and chatbot with transparent, source-linked answers

Cyber rapid risk assessments

Systems-of-systems approach to evaluate cybersecurity risks across digital energy and industrial systems; assigns cyber criticality scores to prioritize components requiring attention

MORE INFO

Cyber rapid risk assessments



SUPPLY CHAIN CAPABILITIES *(CONTINUED)*:

TOPGEAR (Technology, Organization, and Person of Interest Graph Extraction, Analysis, and Reporting)

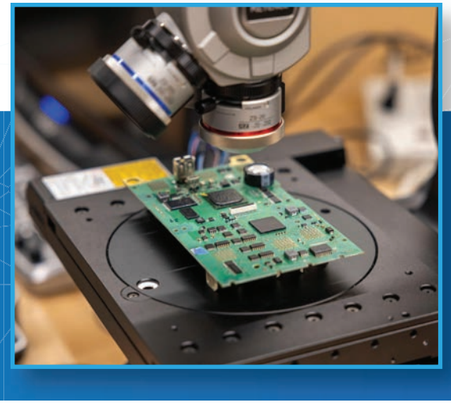
Maps organizational, ownership and vendor relationships to identify risks across critical infrastructure sectors

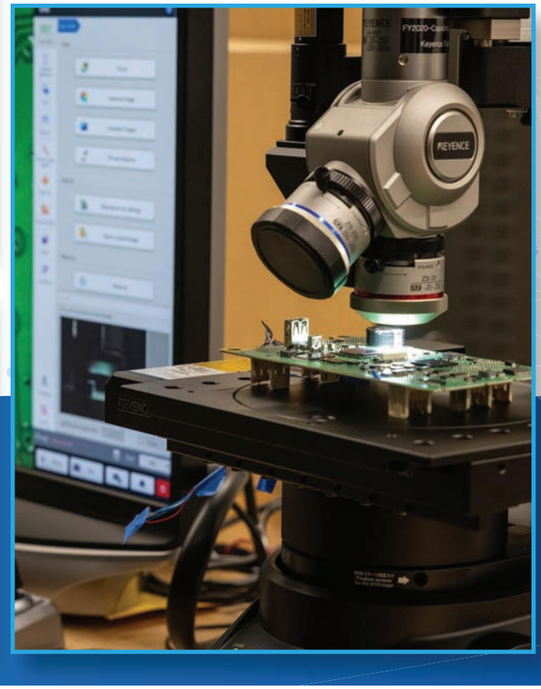
INL develops and evaluates methods to illuminate and secure digital supply chains of critical energy infrastructure

MORE INFO

TOPGEAR

CyTRICS™





5 SUPER INTELLIGENCE/ MACHINE LEARNING SECURITY AND ASSURANCE

INL addresses a critical national need by developing and evaluating super intelligence (commonly known as artificial intelligence) and machine learning (SI/ML) enabled technologies in OT and industrial control systems (ICS) environments. Our software engineering, infrastructure, and applied data science teams build advanced analytical tools, automated risk assessment platforms, and decision support systems that leverage SI/ML to scale infrastructure security analysis.

CAPABILITIES INCLUDE:

- Machine learning models for anomaly detection, predictive maintenance and operational awareness
- Identify SI-enabled vulnerabilities and adversarial attack surfaces
- Secure model development, validation and verification for trustworthy performance
- Apply ML for network traffic characterization, wireless spectrum analysis and signal identification
- Research into next-generation SI/ML challenges including autonomous system security and adversarial ML



SI SECURITY TOOLS:

Cognito

SI-readiness framework helping electric utilities assess capabilities, evaluate risks, and responsibly plan and implement SI solutions

Artificial Intelligence Management and Research for Advanced Networked Testbed Hub (AMARANTH)

Evaluates resilience, performance, and model-drift behavior of high-TRL SI systems in energy-sector operational environments through red-teaming, quantitative analysis, and adversarial testing

MORE INFO

Cognito

SI SECURITY TOOLS *(CONTINUED)*:

Binary Analysis Capability

INL uses advanced machine-learning and graph-based methods to uncover vulnerabilities in compiled code without needing source access

OT Cybersecurity & Threat Analysis

Lab tools strengthen OT cybersecurity by analyzing attack surfaces and improving detection and response to malicious activity across critical energy systems

SI-Driven Risk & Modeling Support

INL applies SI-enabled modeling and risk-assessment techniques to analyze infrastructure, forecast impacts, and support strategic communications

MORE INFO

@DiSCO CyOTE Core II



6 INFRASTRUCTURE HARDENING AND RESILIENT DESIGN

As energy and industrial systems become increasingly digital, traditional cybersecurity alone cannot prevent catastrophic consequences when adversaries breach control systems. INL's infrastructure hardening and resilient design work protects critical operational technology (OT) across power grids, oil and natural gas operations, water treatment, pipelines, and industrial control environments.

INL merges engineering, controls and cybersecurity expertise to design mitigations that enhance the resilience of critical infrastructure systems to cyberattacks. INL strengthens operational systems and enhances their safety and reliability, even while under attack.





RESILIENT DESIGN APPROACH:

Cyber-Informed Engineering (CIE)

An engineering approach that integrates cybersecurity principles into the entire life cycle of critical infrastructure systems, limiting the consequences of cyberattacks and enhancing safety, reliability and resilience. The CIE program also provides outreach to academia and industry across all sectors and OT environments.

MORE INFO



INFRASTRUCTURE HARDENING EXERCISES:

Liberty Eclipse

INL leads hands-on exercises, like Liberty Eclipse, where utilities, cybersecurity professionals, and operational teams can practice detecting, responding to, and recovering from realistic cyberattacks on the power grid — all within a safe, controlled environment. Designed for industry, these exercises strengthen coordination, preparedness, and real-world resilience.

MORE INFO

TECHNICAL ASSISTANCE:

INL provides technical assistance in infrastructure hardening to qualifying asset owners, state and local organizations, energy sector vendors, etc.



7 STAKEHOLDER PREPAREDNESS AND TECHNICAL ASSISTANCE

INL strengthens national, state and local preparedness through its critical infrastructure, cybersecurity and engineering expertise. Technical assistance helps stakeholders make risk-informed decisions and shape policies that improve security and coordinated response. INL experts also inform policy by providing expert testimony to state and federal officials, helping decision-makers understand emerging risks and effective resilience strategies. Tailored assessments and mitigation planning provide clear insight into risk posture, dependencies and protection strategies.







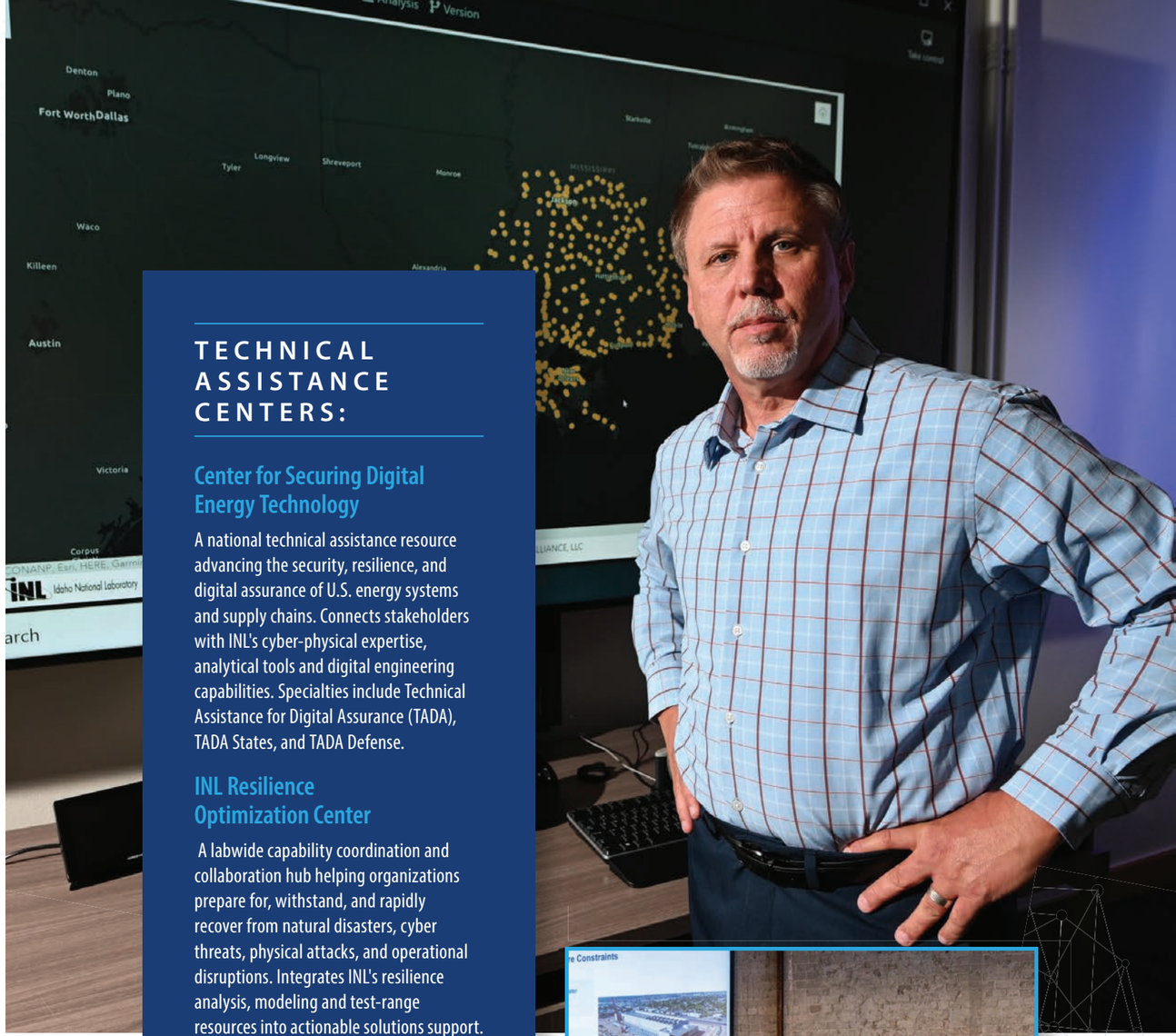
TECHNICAL ASSISTANCE PROGRAMS:

Operational Technology Defender Fellowship

INL provides technical assistance through a variety of programs, including the OT Defender Fellowship. OTDF is a year-long, INL-hosted program that equips OT security leaders across the energy sector with strategic awareness, interagency insight, and hands-on experience defending critical infrastructure.

MORE INFO

OT Defender Fellowship



TECHNICAL ASSISTANCE CENTERS:

Center for Securing Digital Energy Technology

A national technical assistance resource advancing the security, resilience, and digital assurance of U.S. energy systems and supply chains. Connects stakeholders with INL's cyber-physical expertise, analytical tools and digital engineering capabilities. Specialties include Technical Assistance for Digital Assurance (TADA), TADA States, and TADA Defense.

INL Resilience Optimization Center

A labwide capability coordination and collaboration hub helping organizations prepare for, withstand, and rapidly recover from natural disasters, cyber threats, physical attacks, and operational disruptions. Integrates INL's resilience analysis, modeling and test-range resources into actionable solutions support.

MORE INFO

Center for Securing Digital Energy Technology

INL Resilience Optimization Center



INTEGRATED INL ENABLERS

World-class technical expertise and trusted partnerships across government, industry, national labs and academia position INL to address the complex challenges of national infrastructure security and resilience.

WORLD-CLASS EXPERTISE

- Cybersecurity and OT/ICS security
- Data science and applied SI/ML
- Power systems engineering
- Modeling and simulation
- Nuclear cybersecurity and integrated energy
- Critical infrastructure security across multiple sectors
- Electrical engineering and software development
- Computer systems administration and application integration
- Technical instruction and integration strategy

TRUSTED PARTNERSHIPS

Government

Collaboration with the U.S. Department of Energy, Department of Homeland Security, Department of War and state agencies

National labs

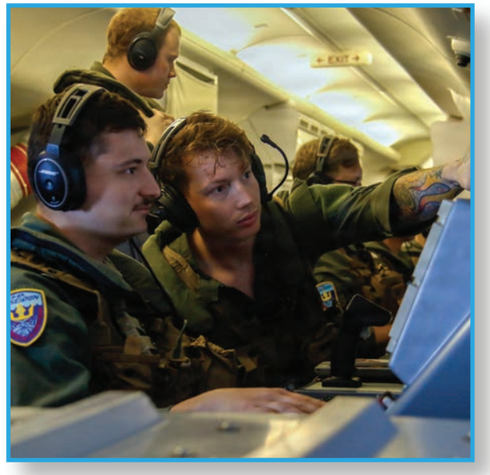
Expertise sharing with partner national laboratories on high-impact research, development, testing and evaluation

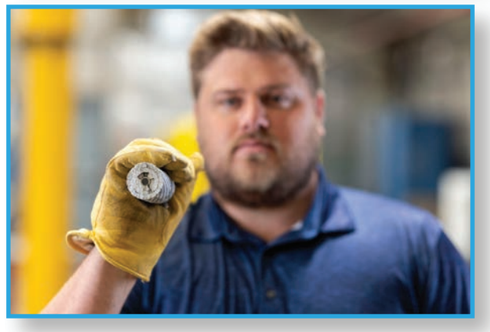
Industry

Guidance and risk-mitigation with vendors, asset owners and operators across critical infrastructure sectors

Universities

Applied research to connect learning with national goals and strengthen workforce development









FOR MORE INFO, VISIT:

INL.GOV/NATIONAL-SECURITY/INFRASTRUCTURE-SECURITY-AND-RESILIENCE

25-50253_05_R6

INL.GOV

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory