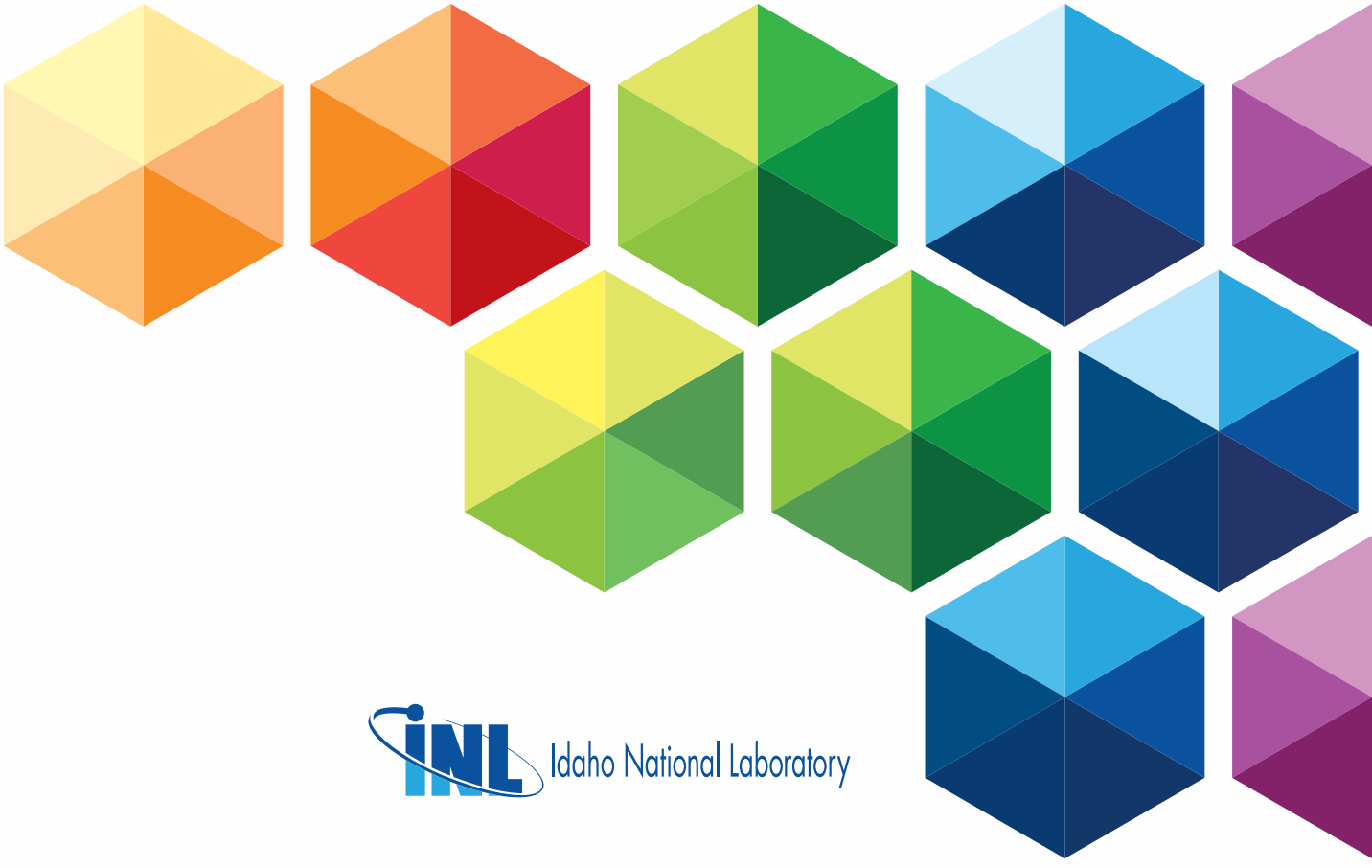
May 2021

CAPABILITIES CATALOG

National & Homeland Security Directorate

Infrastructure Assurance & Analysis Division



Idaho National Laboratory

CONTENTS

BACKGROUND

Idaho National Laboratory (INL) is a recognized leader in creating a more secure and resilient world through innovative infrastructure-related solutions.

INL's national security experts are widely recognized for securing critical digital systems and improving infrastructure resiliency. It is our goal to create a secure and resilient world to support economic prosperity, health, and defense.

INL is uniquely positioned at the nexus of cyber-physical, information and operational technology (IT/OT) convergence, and infrastructure dependencies and interdependencies to address the exponentially growing risks to our Nation's critical infrastructure.

Employing a collaborative approach at INL allows us to address challenges in a comprehensive way. We have a vast network of subject matter experts, access to full-scale infrastructure testbeds, and a strategic center that enables world-class solutions to be developed for the Nation's greatest infrastructure challenges.

INL'S INFRASTRUCTURE ASSURANCE AND ANALYSIS SOLUTIONS FOCUS ON THREE PILLARS:

Infrastructure Analysis | Cyber Resilience | Workforce Development & Training

CATALOG OVERVIEW

This Capability Catalog provides a high-level overview of INL's infrastructure assurance and analysis solutions in support of the National and Homeland Security mission. These capabilities are summarized in the three following categories:

Infrastructure Analysis

INL's critical infrastructure analysis enables stakeholders to improve resilience and disaster preparation through resiliency assessment, dependency analysis and visualization, commodity and proportional flow mapping, modeling, and geospatial analysis, as well as tabletop exercises and other risk management tools.

Cyber Resilience

INL advances the cyber resiliency of critical infrastructure systems for the U.S. through improving and supporting cyber-physical risk analysis and risk management based on IT/OT cyber defense and digital engineering practices. The cyber resilience capabilities are focused on evaluating cyber risk to critical infrastructure and creating systems architectures that mitigate risk and increase the cyber resilience of the nation.

Workforce Development and Training

INL directly supports the Nation's efforts to develop a more efficient cybersecurity talent pipeline through collaborative work with government agencies, private sector businesses, and academic entities from multiple states. INL leads work groups to tackle tough educational issues, as well as designs, develops, and delivers individual training courses to meet specific customer needs and enhance infrastructure resilience.

INFRASTRUCTURE ANALYSIS

INL supports a host of infrastructure security and resiliency missions across federal, state, and local governments and the private sector. Our staff have been hand-picked from nationally recognized subject matter experts in infrastructure security and resiliency, mission assurance, emergency management, intelligence, and lifeline infrastructure operations, and include scientists, academics, modelers, developers, and geospatial experts to support groundbreaking and national laboratory-level innovations in support of our customers. Our portfolio of work includes technical, assessment, cascading and dependency analysis, and software-based solutions, in addition to artificial intelligence (AI) and machine learning (ML) and use of our supercomputing resources to support rapid and efficient methods for solving complex infrastructure-related questions. Our team consists of recognized leaders in real-time risk-informed critical infrastructure analysis who support emerging and ongoing emergencies and longer-term strategic decisions, policymaking, and investment decisions.

Infrastructure Studies

Critical infrastructure analysis enables stakeholders to improve resilience and disaster preparation through resiliency assessment, dependency analysis and visualization, commodity and proportional flow mapping, modeling and simulation, and geospatial analysis, workshops, and risk management methodologies and tools.

Cyber-Physical Consequence Analysis

Cyber-physical consequence and interdependency analysis are being developed to identify risk reduction measures, train national and homeland security workforces, and provide a new framework for examining vulnerabilities in operational technology. This complements cybersecurity and electric test bed capabilities, bridging the gap between cyber- and physical-interdependency analysis.

Risk and Decision Analysis

Risk and decision analysis informs stakeholder decision making to support emergency response, hazard preparation, infrastructure resilience, and cyber-physical security. These techniques enable informed decision making through applying advanced simulation and modeling capabilities and expertise with the goal to mitigate risk and enhance infrastructure resilience.

Comprehensive Resiliency Analysis

Comprehensive resiliency analysis applies advanced analytic techniques and exercise development to better understand critical infrastructure interdependencies, improve partnerships between infrastructure owners and operators, and enhance regional resilience. These efforts support stakeholder decision making by providing resilience assessments that characterize both cyber and physical systems and supply chains.

Infrastructure Systems Characterization
Infrastructure systems characterization, such as the development of infrastructure dependency profiles, groups systems through engineering design principles and helps identify relationships between systems. This reveals the possible system dependencies which inform dependency profiles that are used as guides for analysts or ML algorithms to evaluate dependency relationships within infrastructure systems.

Emergency Management Planning, Response, and Recovery

Emergency management planning, response, and recovery increases the resilience of mission essential functions through continuity planning. This involves staff deployment for data collection and infrastructure stabilization, dependency analysis, and all hazards analysis integration. Subject matter experts create mission decomposition analyses and support, mitigation evaluations, and mission assurance reports to increase stakeholder knowledge of planning and response best practices.

Geospatial Science Analysis and Custom Visualization

Geospatial science analysis focuses on deriving conclusions about physical and operational aspects of critical infrastructure through the analysis of spatial information. This employs remote sensing, geographic information systems, and global positioning techniques to collect and manage the Nation's critical infrastructure data. INL creates custom interactive maps, graphics, and visualizations and employs the Sync Matrix Tool for data-driven incident planning.

Infrastructure Applications Information Technology Architecture Design and Software Development

Custom IT architecture design and software development for infrastructure applications serves to solve complex challenges in critical infrastructure protection. These innovative applications are developed using modeling and simulation, information system analytics, and host data. Subject matter experts administer these certified applications and safely handle protected critical infrastructure information, sensitive regulatory, and proprietary data.

Intelligence-Informed Infrastructure Analysis

Intelligence-informed infrastructure analysis increases stakeholder understanding of infrastructure vulnerabilities by collecting and analyzing data from open and closed sources. This analysis is used to formulate business-related and unclassified intelligence to inform stakeholder decisions and planning for all-hazard threats.

Risk-Informing Infrastructure Analysis

Risk-informing infrastructure analysis addresses all hazards impacts to infrastructure, informs security decisions, and strengthens system resilience. INL employs vulnerability assessments, consequence analysis, the All Hazards Analysis (AHA) tool, and

simulated infrastructure attacks to provide in-depth understanding of infrastructure gaps and the methods to mitigate them. Analysts focus on all 16 Department of Homeland Security designated infrastructure sectors, to include a burgeoning focus on the Healthcare and Public Health Sector.

Modeling and Simulation, Artificial Intelligence, and Machine Learning

Critical Infrastructure-Related AI/ML Applications

Critical infrastructure AI and ML enable computer systems to perform tasks like visual perception and decision making. INL is developing new AI and ML applications that will identify and classify critical infrastructure facilities from satellite imagery and use advanced web crawling to summarize information useful for understanding potential cyber weaknesses.

Scientific Computing

By leveraging INL's onsite supercomputers, tough resiliency calculations can be completed faster and more efficiently. Scientific computing supports projects that seek to eliminate and reduce risk to infrastructure investments, focusing on resiliency of systems and supply chain modeling. This helps reduce risk and enhance knowledge of system behavior through the creation of resilience design evaluations, large-scale vulnerability analyses, and mitigation testing.

All Hazards Analysis

AHA applies enhanced modeling and simulation techniques for hazard and impact analysis to improve stakeholder understanding of vulnerabilities and resilience issues in infrastructure systems. These analyses help identify effective risk reduction measures and provide valuable insights, awareness, and warnings from a live system that demonstrate dependencies and the ebbs and flows of supply and service.

Supply Chain Analysis and Optimization

Supply chain analysis and optimization aims to increase stakeholder knowledge of supply chain system behavior through modeling, simulation, and decomposition, while securing reliable materials, transportation, and backups. INL's comprehensive analysis is presented through custom diagrams, reports, and resilience options to increase understanding and improve resilience of supply chains.

CYBER RESILIENCE

In a digitally engineered and converged world, INL strives to be the Nation's leader in architecting and improving converged cyber-secure systems that provide for robust data and process survivability, redundant means of functioning, and resourceful methods to diagnose and prioritize problems and engineer rapidly recoverable critical infrastructure.

Cyber-Defense Operations and Incident Response

Cyber-Defense Operations and Incident Response assesses organizational security using proactive and reactive searches for malicious activity. After a system analysis, INL provides technical remediation and intrusion detection recommendations, training, and guidelines for implementing incident response capabilities.

Cyber Incident Response and Recovery
Cyber Incident Response targets malicious cyber activity and crises within the pertinent domain to mitigate immediate and potential threats. INL uses network and host forensics to capture and analyze security attacks to coordinate incident response with response and recovery approaches.

Threat Hunting and Analysis
Threat hunting is the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.

Incident Response Capabilities Development
Incident Response Capabilities Development uses incident assessments and analysis to develop and integrate custom cyber response kits that enable rapid response to threats. INL's cyber response kits use signature and anomaly-based detection to successfully prepare systems against threats.

Incident Response Planning and Preparedness
Incident Response Planning and Preparedness determines the best practices in incident response, integrates practices into the planning process, and coordinates response training and exercises. INL analyzes and reimagines response policies to strengthen incident planning and preparedness for organizations.

Cyber-Defense Operations
Cyber-Defense Operations collects information from open and closed sources to identify, analyze, and report events that have occurred or might occur within the network. This information is used to apply defensive measures and protect information, systems, and networks from threats.

Cyber Architecture Risk Evaluation and Mitigation

Cyber Risk Evaluations are conducted to understand system and network vulnerabilities and determine risk levels through onsite analysis, recurring system scanning, and vulnerability analysis. INL develops recommendations through analysis findings of exploitable vulnerabilities to help organizations apply the appropriate mitigation measures.

Critical Infrastructure Cyber Assessments and Risk Analysis
Critical Infrastructure Cyber Assessments and Risk Analysis analyzes critical infrastructure assets to identify system threats and vulnerabilities. INL assessments of cyber maturity, OT and IT, regional resiliency, and macro- and microsystems assist asset owners in mitigating risk and formulating policy and research priorities.

Assessment Methodology Development
Assessment Methodology Development develops and enhances tools and methods to improve assessments of system and network vulnerabilities. The tools and methods are developed using research, information on identified vulnerabilities, and cybersecurity analysis to support vulnerability analysis of systems and networks.

Expert Review of Network and Systems Architecture

Expert Review of Network and Systems Architecture provides feedback on best practices, policies, and potential impacts on existing network architecture of industrial control and integrated cyber systems of critical infrastructure assets. INL's team conducts design architecture review, network architecture validation, and verification, and assessments on risk and design to strengthen an organization's existing architecture.

Cybersecurity Risk Management Framework Development

Cybersecurity Risk Management Framework Development helps asset owners understand and develop a strong risk management framework. Using INL programs, policy development tools, and industry best practices, critical infrastructure owners build and manage a strong cybersecurity foundation.

Vulnerability Management and Coordination

Vulnerability Management and Coordination allows critical infrastructure owners and operators to understand, report, and solve vulnerabilities. INL works with stakeholders to assess potential vulnerabilities, identify possible remediation solutions, and support the implementation of those solutions.

Vulnerability Verification and Validation

Vulnerability Verification and Validation analyzes identified system vulnerabilities to determine the level of associated risk. Vulnerabilities that present validated risks can be addressed properly.

Vulnerability Remediation

Vulnerability Remediation is the process of addressing validated vulnerabilities through patching and applying improved system cybersecurity scans and measures.

Critical Infrastructure Trend Analytics

Critical Infrastructure Trend Analytics give researchers and infrastructure stakeholders a better understanding of trends and best practices in infrastructure vulnerability identification and remediation.

Digital Engineering Design and Architecture

INL applies digital engineering principles to build and maintain the cybersecurity of critical infrastructure. INL employs advanced infrastructure hardware, software, and system knowledge to manage network defense services and actively remediate unauthorized activities.

Cyber-Defense IT Architecture and Design

Cyber-Defense IT Architecture and Design uses IT automation and systems integration to design stronger cyber-defense infrastructure. INL provides secure design and integration services into cyber-physical testing ranges.

Cyber-Defense Infrastructure Research

INL's Infrastructure Research is conducted with special focus on system innovation and resilience integration. This research informs cyber-defense infrastructure design and strengthens testing capabilities.

Cyber Systems Support

Cyber Systems Support is the process of designing systems and networks to support testing and research findings. INL uses data warehousing to manage and secure a high volume of cyber-defense infrastructure information from many sources.

WORKFORCE DEVELOPMENT AND TRAINING

INL creatively utilizes instructional systems design models to develop and deliver cybersecurity educational products and experiences in which today's workforce can benefit. Many learning environments (classroom, hands-on, eLearning, mixed reality, exercises, etc.) are considered when designing courses to facilitate efficient and effective knowledge transfer of materials. INL focuses on developing curriculum for infrastructure owners and operators related to topics, such as cyber and physical security, infrastructure dependencies and interdependencies, resilience, and risk.

INL trainings are delivered in fully immersive laboratory settings providing constructive experiences based on realistic industry job roles and functions. This allows students to immediately use knowledge applicable in their daily jobs. Mobile courses provide scaled-down experiences, and incorporate control system kits for similar hands-on learning experiences. Virtual (eLearning) courses convey curriculum using a variety of delivery systems, such as webinars, self-paced modules, and virtual exercises, that simulate tasks and experiences linked with actual training equipment located in INL's laboratories.

INL is assisting multiple organizations with the creation of a cybersecurity workforce development and education pipeline. This pipeline combines identifying and adopting educational IT and OT cybersecurity standards for academia, a means to assist entities with identifying training and education needs that match their employee's roles and responsibilities, and establishing a collaborative community of stakeholders that exchange new ways to address issues in the rapidly changing cyber-threat landscape.

Cybersecurity Training Delivery

INL applies proven delivery methods for training courses to participants from around the world, with both unclassified and classified options. Course designs are influenced by the method of delivery desired by each customer and employ immersive classroom settings using adaptive static or mobile equipment that emulate industrial control systems (ICS). Often a train-the-trainer component is incorporated into courses. These courses can then be distributed to customers to conduct their own course instruction while continuing to leverage INL expertise when needed.

Tailored Cybersecurity Training Instructional Design for Formal, Mobile, and eLearning

The Instructional Design Section capability analyzes and solidifies a customer's training requirements, designs and develops course curriculum, implements the course with instructor staff, and evaluates coursework for improvement. Based on the identified need, courses incorporate different learning environments, such as live, virtual, constructive, and gaming, to maximize the student's experience and knowledge transfer. A variety of training aids can be incorporated into the design based on customer requirements.

ICS Cybersecurity Training Aids Development

INL experts and engineers collaborate to build training aids designed to meet course requirements and best capture desired curriculum intent.

International Association for Continuing Education and Training Accredited Curriculum

INL can provide Continuing Education Units for INL developed courses or existing courses that are retrofitted to established IACET guidelines.

Training aids can be developed as stand-alone components, or as part of a multifaceted system. These training aids are tailored to maximize the student's experience and knowledge gained. INL's legendary hands-on experiences set in realistic work environments allow students to apply the necessary tools taught in the classroom to defend control systems. Training aids and scenarios also showcase potential impacts on control systems due to unaddressed vulnerabilities in a safe setting with no risk to any production systems.

Cyber-Cybersecurity Competency Health and Maturity Progression (Cyber-CHAMP©) Diagnostic Model

There is a need to increase the ICS Cybersecurity workforce's access to the necessary education and resources to improve their workplace competency. Many organizations are uncertain of their workforce's continuous educational needs that enable employees to sustain a secure cyber environment within their organization. Furthermore, if an organization has attempted to create a cybersecurity training plan, it is most likely not broken down by defined cyber-job roles or functions. The CYBER-CHAMP© diagnostic model identifies current ICS cybersecurity competencies in five key areas and outlines a roadmap for employee cyber-skills improvement through attending the appropriate cybersecurity training and not just a course randomly picked out of a catalog. The diagnostic model used within an organization results in a workforce education and training profile that details current and future needs, analysis on the educational state of their cybersecurity workforce, learning paths created by role, and a continuous improvement program to stay abreast of necessary training based on the ever-changing threat landscape.

FINAL THOUGHTS

Our capabilities enable us to work towards our vision: A secure and resilient world to support economic prosperity, health, and defense. We are dedicated to advancing our research and development, creating and implementing innovative solutions to the most challenging infrastructure problems, and aligning to a strategy that strives to increase security and resilience through infrastructure workforce development and training, infrastructure analysis, cyber resilience, and workforce development and training.

For more information:
iaa@inl.gov

inl.gov
inl.gov/national-security
resilience.inl.gov

Idaho National Laboratory

21-50121-R3