State Technical Assistance for Digital Assurance

How States Can Drive Digital Assurance Outcomes and INL's Path to Support

States and state agencies play a pivotal role in policy leadership as well as ensuring the reliability, resiliency, and security of the electrical grid.

States control funding, provide guidance and assistance, and set requirements. State offices departments, and public utility commissions by participating in a TA engagement to enhance the cyber maturity of state energy programs and policies.

INL Technical Assistance for Digital Assurance (TADA) States:

Goal: Enhance digital assurance and risk reduction in the deployment of modern energy infrastructure across U.S. states and suppliers.

- Help states with managing and mitigating risks from digital energy equipment through technical assistance, training, and strategic analysis.
- Provide tools to states to effectively evaluate vendors, infrastructure investments, and geographic risk factors.
- Conduct workshops, working groups, and provide direct technical support to help mitigate risks associated with non-domestic supply chains and strengthen national security.

What Can States Do?

Secure, resilient energy infrastructure is essential for grid capacity growth and modernization. States play a key role by guiding energy stakeholders, directing infrastructure funding, and setting requirements for grid expansion and operation. To support these efforts, the Department of Energy has funded Idaho National Laboratory (INL) to provide states with direct technical assistance through tailored digital assurance capabilities.

Specific actions states may take:

Promoting energy policy goals and initiatives

Defining interconnection and grant criteria

Reviewing system and vendor designs for safety and performance

Incorporating cybersecurity and resilience expectations into state programs and procurement calls

Coordinating with utilities and applicants to verify CIE-based risk mitigation

Tracking outcomes to improve state energysecurity planning

States have capacity to influence digital assurance for the electric sector:

States can design procurements to favor awardees who describe/demonstrate **high cyber maturity**

States can set **independent** requirements or **integrate digital assurance** with a cybersecurity plan

State roles and organizational structures vary. Use cases can be **adapted** based on **specific needs and capabilities**

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

INL Idaho National Laboratory

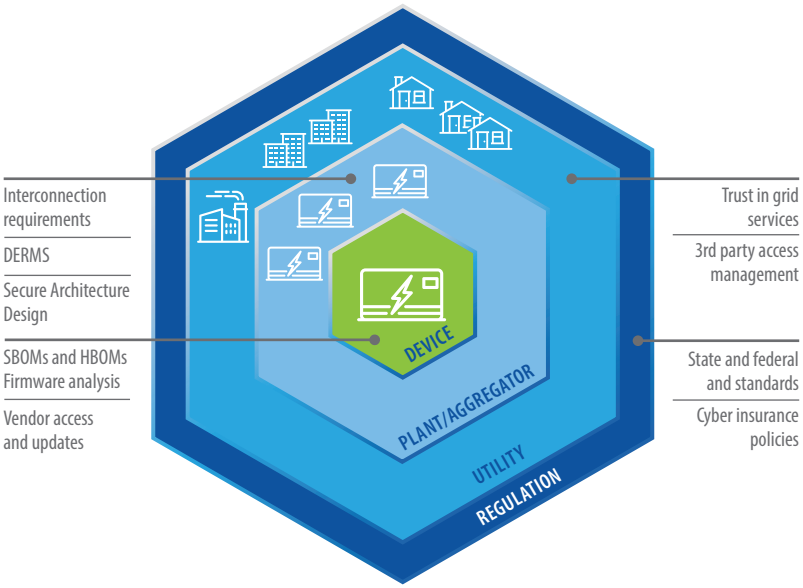
Where Do We Start?

INL subject matter experts strengthen state energy infrastructure by securing supply chains through policy and risk analysis.

Who's eligible?

- State Energy Offices
- Emergency Coordinators
- Energy Managers *(and related offices)*
- Public Utility Commissions
- Tribal Offices *(addressing energy security and resilience).*

Related offices are eligible for TA through this program



Implementing the Technical and Policy Measures That We Already Have

Solutions, analysis, and research MUST take a system-of-systems approach to reduce risk

There is no fast path to economically eliminating supply chain risk and non-domestic dependencies

Most direct approach is implementing a Cyber-Informed Engineering (CIE) approach to secure systems and mitigate risk

Optimize Supply Chain → **Inspect It** → **Operate Through Risk**

Navigating Digital Assurance Challenges

Building Resilient Systems for Electric Grid Modernization

Policy & Education	Technical Tools	Digital SCRM
Tailored Threat Briefs	Harden State and Local Interconnection Requirements	Organizational Influence Analysis and Visualization
Tabletop Exercises (TTX) for Incident Response	Risk-aware Procurement and Contract Language	Labeling Requirements at the State Level
Cyber-Informed Engineering (CIE) Education	Development or Review of Draft Guidelines	Vendor Risk Evaluations
Hands-on Security Training		Software Bill of Materials (SBOM) Hardware Bill of Materials (HBOM)
Support Relationship Building		

Education - Knowledge of Cyber Risk

Threat Briefs

- Energy-sector threat trends and emerging adversary behaviors
- State-level risk profiles aligned to energy mix and system vulnerabilities

Technology Discussions

- Performance contraints and cyberattack surfaces
- Stakeholder networks

Supply Chain Risk Deep Dives

- Geographic, vendor, and geopolitical risk concentrations
- Critical component vulnerabilities

Tabletop Exercises and Workshop Support

Tabletop Exercises (TTX) Support Real-World Learning and Relationship Building

- Bring together stakeholders from
- Identify roles, contacts, procedures, and where gaps exist
- INL provides session facilitation, planning support

Incident Response Guides

- Focus on roles and responsibilities, event and incident identification and classification
- Review best practices and walk through incident preparedness scenarios
- Cross-sector relationship building

Support for Information Sharing Frameworks

- National resources and organizations
- Mutual support mechanism to use within a region
- Resources for cyber threat intelligence sources

Cyber-Informed Engineering (CIE) Education

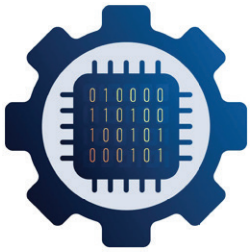
What is CIE?

CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.

CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.

Focused on **engineers and technicians,** CIE provides a framework for cyber education, awareness, and accountability.

CIE aims to create a **culture of security** aligned with the existing industry safety culture.



CIE for States Package: Provides state-focused CIE tools for grantmaking, interconnection, device approvals, and training

CIE Introduction: Purpose, Why CIE, Benefits of CIE, How SEOs Advance CIE, CIE Principles

State-Focused Use Cases: State Funded Grants, Training and Development, Interconnections, Allow Lists

Tools and Templates: CIE Grant Scoring Rubric, Impact Assessment Tools, Future Additional Use Cases, "Day Without Automation"

Note: Technical CIE tools for asset owners can be provided upon request. CIE Engagements can be provided in-person, online, or at large events/conferences.

Hands-on Security Training

Training supports workshop development, informs policies and procedures, builds a culture of awareness

Cyber-Informed Engineering

- Introduction to CIE, use cases and tool demonstrations

CyberStrike STORMCLOUD

- Hands-on hardware kit with red team and blue team operations

Escape Rooms

- Gamify security concepts in an interactive environment

Time Commitment

- Each workshop may be 1-8 hours in length
- Consultation before and qafter training

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

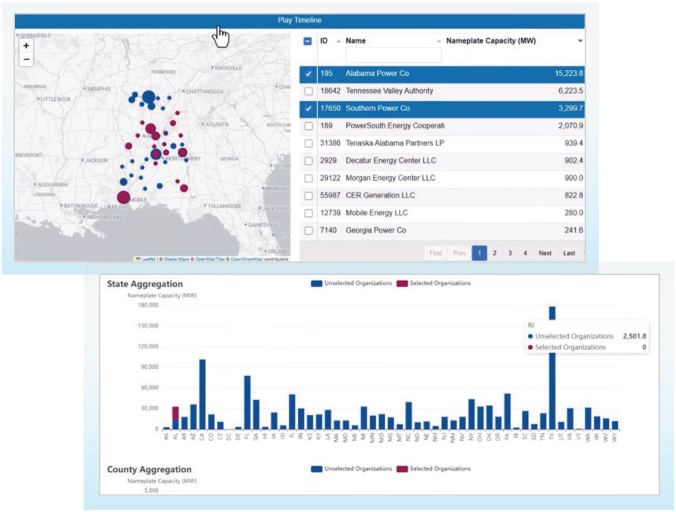
Practical Objective:
Address Ownership, a vital supply chain risk analysis gap given its potential for long-term legal, but adversarial influence.

Description:
Risk analysis based on regional energy profiles and risk factors

- Generation mix and projected changes + Impact of large loads

Supply chain and influence analysis visualization

- With vendor penetration data and prioritization of risk exposure
- Direct and indirect influence assessment



Value for States
Visibility: geospatial interface to visualize and monitor current and possible organizational influence on regional systems.

Prioritization: Investigate regional supply chain ownership risks including data provenance, common-mode failures, and M&A

Get Started

For more information:
https://inl.gov/csdet-technical-assistance-and-training/

Scan to Apply Now:

For more information
Megan Culler
208-526-7761
megan.culler@inl.gov.

25-50904_R01
INL/MIS-25-84987