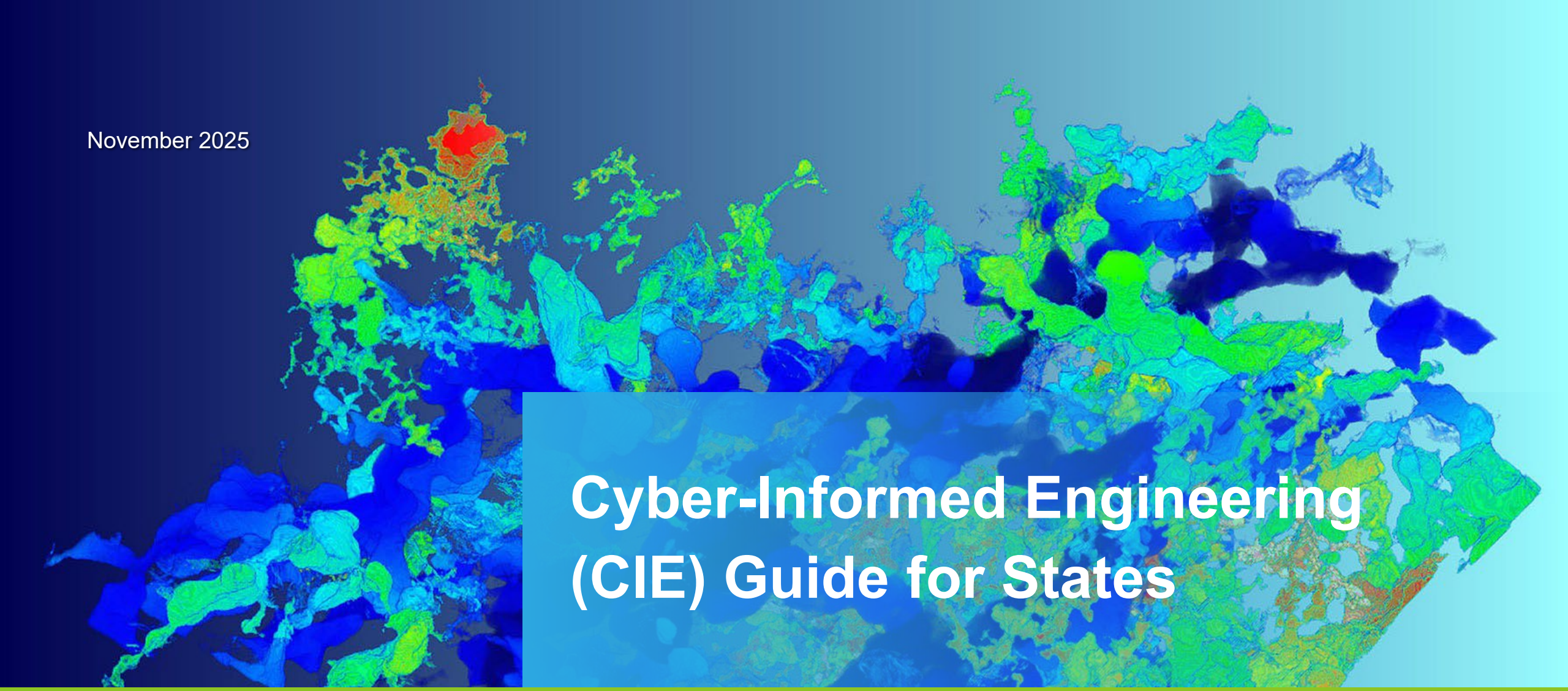
November 2025



Cyber-Informed Engineering (CIE) Guide for States

INL/MIS-26-90828

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

Idaho National Laboratory

CONTENTS

1. **Introduction to CIE in States**
   - A. Purpose
   - B. Why CIE Now
   - C. Benefits of CIE
   - D. How SEOs Advance CIE
   - E. CIE Principles
2. **State-Focused Use Cases**
   - A. State Funded Grants
   - B. Training and Development
   - C. Interconnections
   - D. Allow Lists
3. **Appendices: Practical Tools & Templates**
   - A. CIE Grant Scoring Rubric
   - B. Impact Assessment Tools
   - C. Future Additional Use Cases
4. **Appendices: Other Use Cases**
   - D. Qualitative Criteria
   - E. Risk Assessment and INL Assistance
   - F. Day Without Automation

Section 1- Introduction

CIE and Its Application by States

Purpose and Sponsorship

Purpose of this Kit

- **Provides** state-focused CIE tools for grantmaking, interconnection, device approvals, and training
- **Packages** INL/NREL research into usable playbooks, rubrics, and exercises

Sponsorship

- **Activities sponsored** by DOE Grid Deployment Office (GDO)
- **CIE rubric development** supported by DOE CESER with INL/NREL

Disclaimer

Federal disclaimer (no warranty, no endorsement of products)

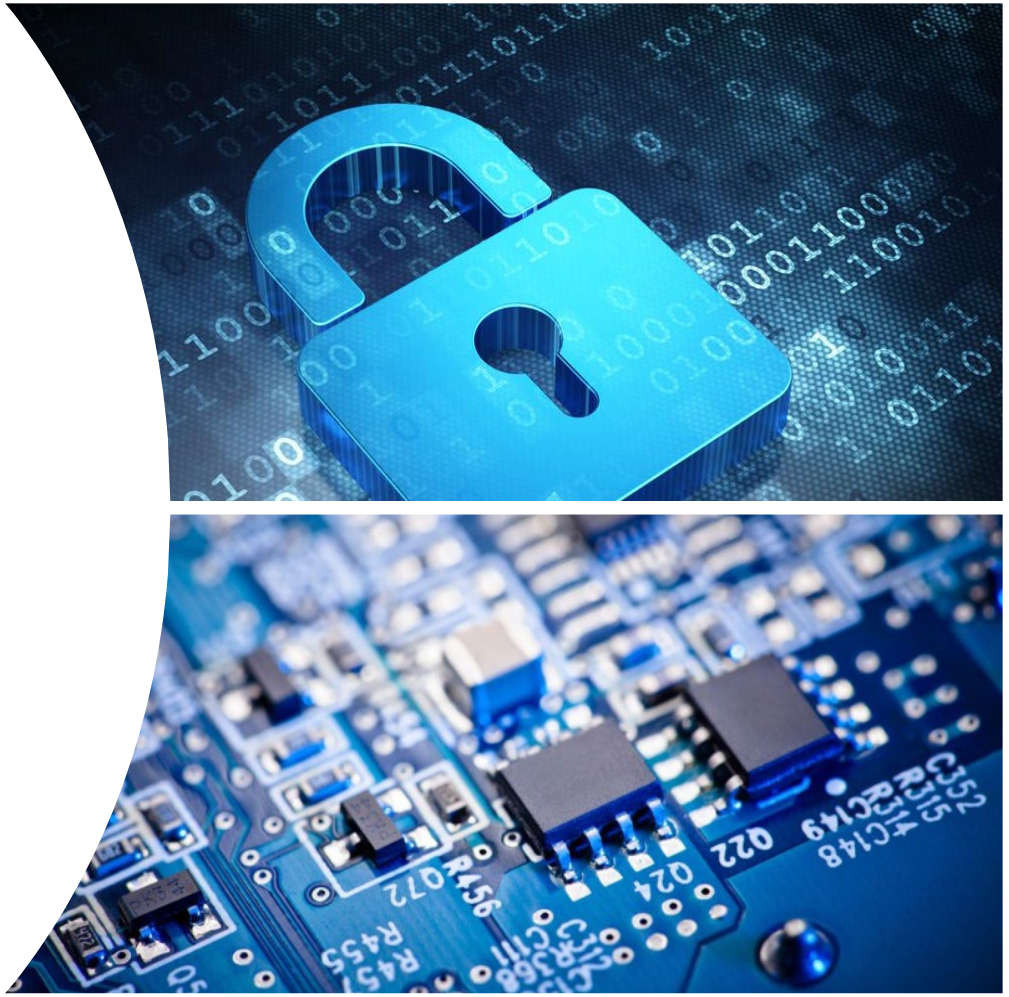
What is Cyber-Informed Engineering (CIE)?

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.



Why Cyber Informed Engineering (CIE)?

The increase of grid digitalization and distributed energy resources (DER) adoption exposes new attack surfaces and increases cybersecurity risks.

Change		Impact to Digital Risk
Expanding ecosystem	→	Supply chain vulnerabilities, vendor dependencies, and data sovereignty risks
Proliferating endpoints	→	Expanded attack surface requiring comprehensive vulnerability management
Critical load transformation	→	Systemic grid impacts from single-point compromises
Evolving governance	→	Complex audit requirements and standards harmonization
Digital control evolution	→	Need for resilience, fail-safes, and role-based access controls
Smarter inverters	→	Expanded attack surface

Why Now for States?

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

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

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

Tracking outcomes to improve state energy security planning

States have flexibility in applying CIE

- States administer energy grants to utilities and applicants from **multiple funding sources**
- CIE can be an **independent** requirement or **integrated** with a cybersecurity plan
- State roles and organizational structures vary. Use cases can be **adapted** based on **specific needs and capabilities**

Who Is This Kit For?

1. State Energy Offices (SEOs)

Leadership, policy, planning, and programs

2. Public Utility Commissions (PUCs)

Regulatory oversight

3. National Associations (NASEO, NARUC)

Standardization and peer learning

Why this audience matters: These groups shape state energy policy and implementation. By embedding CIE into their workflows, they can:

- **Set** policy direction
- **Support** smaller utilities and co-ops with technical assistance and training
- **Coordinate** with other state agencies (e.g. emergency management)
- **Incentivize** cyber-resilient design across programs

Benefits for States of CIE

By incorporating "secure by design" principles, CIE represents a philosophical shift in how state operators manage the grid. This can realize a range of benefits.

How CIE changes the operation and management of the grid:

- **Consequence-focused planning**
- **Mindset shift**

Benefits of CIE

- **Increases grid resiliency** by engineering out high consequence events through physical controls
- **Lowers total cost of ownership** by preventing expensive outages and retrofits
- **Supports economic competitiveness** by attracting inward investment encouraged by grid reliability
- **Advances workforce development** by positioning state as leader in cyber-secure operations

How State Energy Offices Can Advance CIE

SEOs are policy leaders who can integrate CIE through multiple pathways.

Strategic Planning

Lead comprehensive energy planning that incorporates digital resilience goals and CIE principles

Example: Add CIE priorities to state energy plan as strategic objective for grid modernization projects

Cross-Agency Coordination

State receives funds and issues RFA with defined topic areas and statutory requirements

Example: Create interagency working group on energy infrastructure security

Policy Frameworks

State receives funds and issues RFA with defined topic areas and statutory requirements

Example: Model legislation to authorize CIE technical assistance and program integration

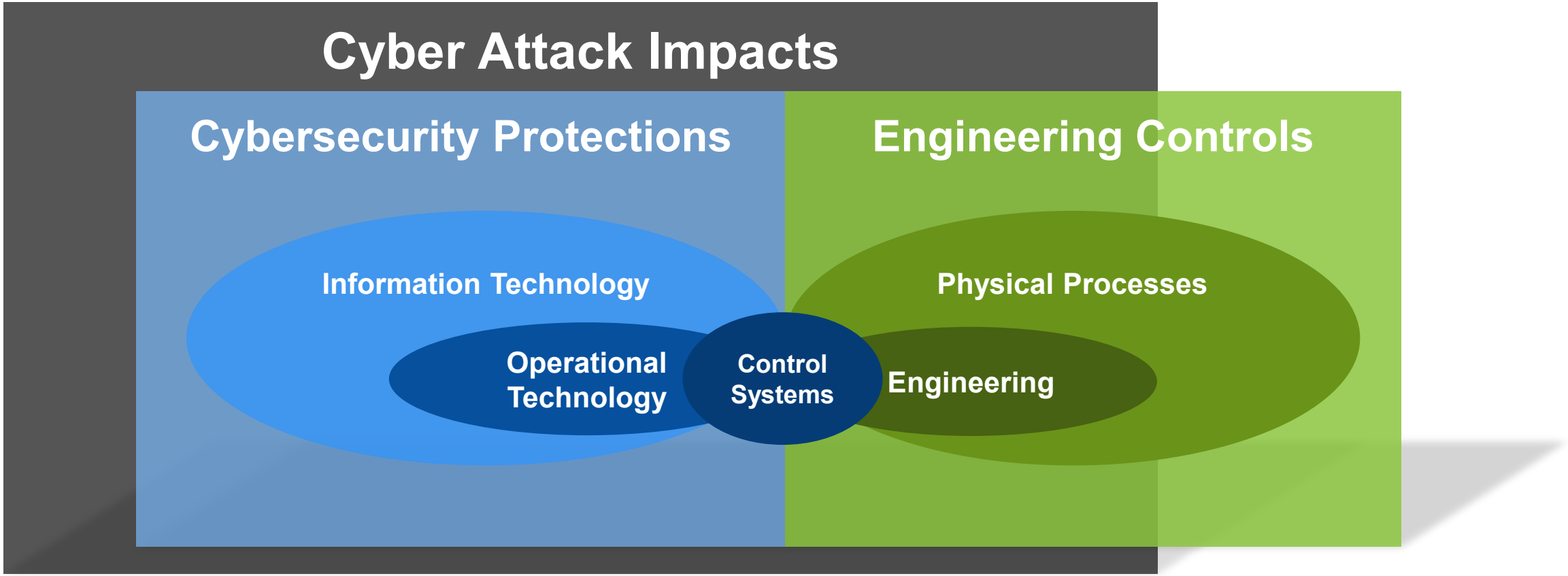
Program Implementation

State receives funds and issues RFA with defined topic areas and statutory requirements

Example: CIE-weighted rubrics in state energy grant programs (see Use Case 1)

CIE use cases focus on tactical implementation tools. These work best when aligned with strategic priorities established through planning and policy coordination.

Cyber-Informed Engineering Introduction



Cyber-Informed Engineering (CIE) Principles

The 12 CIE principles help engineers design systems resilient to cyber risks and consequence failures.

Principle	Question
1. Consequence Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
2. Engineered Controls	How do I select and implement controls to minimize avenues for attack or the damage that could result?
3. Secure Information Architecture	How do I prevent undesired manipulation of important data?
4. Design Simplification	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
5. Layered Defenses	How do I create the best compilation of system defenses?
6. Active Defense	How do I proactively prepare to defend my system from any threat?

Cyber-Informed Engineering (CIE) Principles (Cont'd)

These principles represent a comprehensive approach to "secure by design", encompassing design, control, impact, and organizational considerations.

Principle	Question
7. Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
8. Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and what our assumptions are about how they work?
9. Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security the system needs?
10. Planned Resilience	How do I turn "what ifs" into "even ifs"?
11. Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
12. Organizational Culture	How do I ensure that everyone's behaviors and decisions align with our security goals?

Section 2 - State Focused Use Cases

State Funded Grants

CIE in State Funded Grants

States (e.g., SEOs) integrate CIE into grant evaluations by embedding risk-focused rubrics, bonus points, and pre-award requirements into funding processes.

Funding & RFA Setup

State receives funds and issues RFA with defined topic areas and statutory requirements

Proposal Requirements

Applicants may submit cybersecurity plans with CIE criteria included in RFP Section

CIE Rubric Evaluation

State may choose to evaluate proposals using weighted CIE rubric developed with INL assistance

Award & Pre-Award Negotiations

If used, selected proposals can refine CIE plans through negotiations before final funding

Execution & Reporting

State may track CIE progress metrics with optional INL technical support throughout project

Integrating CIE Requirements into Grant Evaluations

A CIE-adapted rubric provides a structured method to evaluate applicant responses against CIE principles.

CIE Options for Proposal Phase

a. **Mandate CIE:** Require all applicants to include CIE in their proposals
b. **Weight CIE:** Assign CIE a portion of overall scoring (e.g., Proposal 30%, Team 30%, Budget 10%, CIE 5%)
c. **Incentivize CIE:** Award bonus points for demonstrating CIE (e.g., Idaho DEQ Drinking Water Grant)

CIE in Pre-award Negotiations

a. **Outline Requirements:** State notifies awardees before funding
b. **Document CIE:** Awardees include CIE in project plans
c. **Review Plans:** SEO approves or requests revisions
d. **Conditional Funding:** CIE deliverables required for award

See Appendix A for a complete summary of the CIE grant rubric

Integrating Qualitative Criteria into Grant RFPs and Grant Evaluations

Qualitative requirements are included in RFPs as narrative expectations describing missions, critical functions, and reliance on automation.

What is it: Narrative expectations describing missions, critical functions, automation reliance, engineered controls, staffing.

Example: “The microgrid must sustain power to the hospital for 7 days, even if automation is unavailable. The applicant must describe how manual operations will be conducted.”

1. **Identify Project Missions & Critical Functions**: Define critical functions to determine where to apply cybersecurity controls
2. **Digital Awareness**: Be explicit about reliance on automation and digital technologies
3. **Automation Engineering Analysis**: Demonstrate how long critical functions can operate without automation
4. **Engineered Control Awareness**: Require built-in physical/manual safeguards
5. **Active Defense Analysis**: Assess staffing, training, and procedures to respond during degraded digital operations

Qualitative criteria guide applicants to tell the story of resilience. They ensure proposals move from reactive cybersecurity to engineered resilience.

Rubrics and Scorecards

CIE Rubric

12 Principles used as scoring categories
Each proposal scored **1–3 points** per principle:

1 = Minimal / No controls
2 = Partial mitigation
3 = Strong engineered controls & resilience

Example (Engineered Controls):
Q: How are engineered systems dependent on digital tech, and what happens if adversary subverts them?

1 pt: No controls; digital-only reliance
2 pts: Some engineered controls; partial mitigation
3 pts: Manual overrides / fail-safes for all critical functions

CIE Impact Scorecard

Evaluates **potential consequences of cyber incidents** in funded projects

Categories include:

- Safety (public & worker)
- Reliability / Service Continuity
- Financial Loss
- Environmental Impact
- Public Confidence
- Information/Privacy

Used to:

- Compare severity of risks
- Prioritize mitigation resources
- Track progress over time

See Appendices A and B for more information

Section 2 - State Focused Use Cases

Training & Workforce Development

Training & Workforce Development: SEOs

Training and workforce development gives states and utility partners the knowledge and tools to apply CIE principles in their day-to-day work.

Organize CIE Workshops

- Host quarterly or semi-annual sessions for utilities
- Use INL training modules as foundation
- Tailor examples to your state's energy mix

Utility Office Hours

- Provide technical consultation for utilities working on CIE-related projects
- Schedule regular drop-in sessions (monthly or quarterly)

Peer Learning Networks

- Create forums for utilities to share CIE implementation experiences
- Facilitate recurring working groups to discuss CIE challenges and solutions
- Support utilities in piloting CIE approaches and documenting lessons learned

Training & Workforce Development: PUCs

Training and workforce development equips PUC staff, commissioners, and stakeholders to understand, evaluate, and implement CIE principles.

Train Engineering Staff

- Ensure PUC engineers can evaluate CIE components in interconnection studies
- Use CIE Implementation Guide and INL webinars for staff development
- Focus training on identifying digitally induced risks in System Impact Studies

Commissioner Briefings

- Educate commissioners on CIE principles to inform policy decisions
- Frame CIE as an extension of existing reliability and safety standards

Stakeholder Workshops

- Host public sessions to introduce CIE expectations for interconnection applicants
- Provide advance notice to reduce surprises during the application process

Role in Training & Capacity Building for NASEO and NARUC

NASEO and NARUC accelerate CIE adoption through training, peer learning, and standardized guidance for states.

NASEO

- Develop model CIE training curriculum for SEOs
- Host national webinars on CIE implementation
- Facilitate peer-to-peer learning networks across states
- Facilitate case study sharing at annual meetings and webinars

National Association of Regulatory Utility Commissioners

- Create CIE training track at annual meetings
- Publish model PUC orders incorporating CIE
- Coordinate regional working groups for PUC engineers
- Publish case study library showcasing state CIE implementations

Staffing and Resources for CIE Programs

State energy offices and PUCs can scale CIE programs by defining clear roles and dedicating modest staff time to coordination, training, and integration.

Role	Responsibility	Time Commitment	Who Fills This?
CIE Program Lead	Coordinate with utilities, INL, and NASEO/NARUC; oversee pilot projects	0.25-0.5 FTE	SEO technical staff OR PUC engineering staff
Grant Review Coordinator	Train reviewers on CIE rubric; score proposals	0.1 FTE (during grant cycles)	Existing grant program manager
Interconnection Liaison	Work with engineers to integrate CIE into System Impact Studies	0.1-0.25 FTE	PUC staff engineer
Training & Outreach	Organize workshops; maintain utility relationships	0.1 FTE	SEO or PUC communications/outreach staff

Available CIE Resources & Tools

INL and DOE provide technical resources, assessment tools, and support to help states apply CIE principles.

Educational & Training Materials	▪ CIE Implementation Guide ▪ CIE Training Modules
Assessment Tools	▪ CIEBAT assessment tool ▪ CIE Microgrid Tools & Workbooks
INL Technical Assistance	▪ States can request INL support for: – Facilitating initial CIE workshops with utilities – Customizing CIE tools for state-specific contexts – Training state staff on CIE assessment methodologies – Technical review of complex interconnection or grant proposals

Section 2 - State Focused Use Cases

Allow Lists

How States Can Apply CIE Through Allow Lists

Allow Lists help states formalize consequence-based vetting, ensuring only resilient, transparent, and cyber-secure technologies are used.

What it is: An **allow list** is a vetted catalog of technologies or vendors that a PUC has approved for use in grid operations or interconnection projects.

It ensures that only systems meeting safety, performance, and cyber-resilience standards are authorized for deployment.

1. **Develop CIE-based criteria** with safety and performance standards that vendors must meet to qualify for inclusion.
2. **Require vendors to submit responses** describing how their products address CIE principles and engineered protections against cyber-physical risks.
3. **Validate vendor responses** to confirm that design and operational features address credible cyber scenarios and consequence mitigation.
4. **Approve or deny inclusion** of the system or device on the state's allow list based on CIE alignment and technical suitability.

INL can assist by developing CIE questions, reviewing vendor submissions, or performing assessments of technologies.

Section 2 - State Focused Use Cases

Interconnection Requests

Understanding the Interconnection Process

The interconnection process defines how new generators show feasibility, assess impacts, and secure agreements before connecting to the grid.

To enter the queue, a generator must:

- Submit a detailed application
- Place a deposit
- Demonstrate site control (land-use agreements for the project location)

Interconnection Process	Summary of Actions
1 Feasibility Study	Assess technical viability and grid operating risks
2 System Impact Study	Model reliability and engineering impacts
3 Facilities Study	Final engineering design and cost estimates
4 Interconnection Agreement	Define roles and responsibilities, and operational terms
5 Construction and Testing	Build, commission, and verify compliance

Digital Assurance Risk in the Existing Process

Digitalization of grid interconnections introduces new cyber vulnerabilities that current interconnection processes do not comprehensively address.

- System impact studies and interconnection reviews **already use** CIE principles
- Cyber events can now **disrupt operations** (trips, mis-operations, lockouts)
- These risks are **not fully addressed** in today's interconnection process
- CIE embeds **cybersecurity awareness** into these same stages and extends this approach

Interconnection Process	Cyber Risk Observation
1 Feasibility Study	▪ Adequacy of communications and control architecture may not be systematically reviewed
2 System Impact Study	▪ Studies narrowly focused on individual facilities, not aggregated system impacts (e.g. from IBRs)
3 Facilities Study	▪ Opportunity to add cyber-resilient design review and vendor remote access controls
4 Interconnection Agreement	▪ Grid communication security requirements not formalized in agreements
5 Construction and Testing	▪ Configuration security validation not currently included

A CIE Revised Interconnection Process

CIE embeds cybersecurity into existing studies and agreements, ensuring digital risks are identified and mitigated alongside physical reliability.

Outcome of CIE Integration

- Proactive mitigation of digitally induced risks
- More resilient interconnections at lower lifecycle cost
- Stronger assurance for utilities, regulators, and customers

Interconnection Process	New Actions
1 Feasibility Study	**Evaluate** adequacy of communications and control architecture
2 System Impact Study	**Add** grid impact analysis of facility operating alone versus aggregated with additional IBRs
3 Facilities Study	**Incorporate** secure design elements (architecture segmentation, authenticated comms, vendor access restrictions, protection logic review)
4 Interconnection Agreement	**Define** CIE-related roles and responsibilities and mitigations (document risks, assign maintenance/accountability)
5 Construction and Testing	**Validate** that security controls are operational and adequate through secure commissioning and configuration verification

Benefits for States of Including CIE in Interconnections

CIE formalizes consequence-based design, giving states better tools for resilient, transparent, and secure interconnections.

1. Built-in Resilience → Builds systems with fallback modes and fail-safe controls to sustain operations through outages or attacks.

2. Clearer supply-chain visibility → Uncovers third-party and cloud dependencies that affect reliability and security.

3. Stronger state leadership → Aligns with DOE's National CIE Strategy and elevates states' role in energy security.

4. Smarter DER integration → Reduces operational blind spots and prevents technologies that could destabilize local grids.

5. Assured interconnection agreements → Embeds CIE reviews to identify and mitigate high-consequence failure modes.

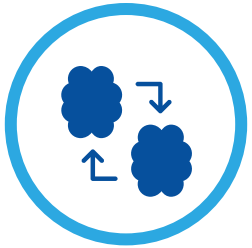
Next Steps for States

States through PUCs can begin applying Cyber-Informed Engineering (CIE) principles through targeted pilots and partnerships.

Pilot CIE in interconnection reviews

Select one or more project to apply CIE methods and document lessons learned.

Build state capacity through CIE training



Train staff on identifying high-consequence failure modes and integrating CIE into interconnection guidelines.

Partner with INL for continued support

Collaborate with INL to expand technical assistance, share outcomes, and strengthen awareness across states.

Section 3 – Appendix A

Grant Rubric

Appendix A – CIE Grant Rubric

CIE Principle	Key Evaluation Question(s)	Scoring		
		1 Point – Needs Improvement	2 Points – Acceptable	3 Points – Exceptional
1. Consequence Focused Design	▪ What high-consequence events could impact mission, safety, environment, or reliability? ▪ How are critical functions mapped to those events?	High-consequence events not defined or not linked to digital systems.	Events partially defined or mapped; unclear digital dependencies.	Clearly defines unacceptable events and ties them to digital functions and critical operations.
2. Engineered Controls	▪ How are systems dependent on digital technologies protected from subversion? ▪ Can failure modes be mitigated via mechanical or manual means?	No engineered controls described; depends solely on digital protection.	Partial or impractical controls; limited feasibility.	Clearly defined, feasible, affordable engineered controls (manual, mechanical, redundant).
3. Secure Information Architecture	▪ Which data exchanges, if disrupted, could cause high-consequence events? ▪ What verifications ensure integrity?	Does not identify critical data exchanges or protections.	Identifies exchanges and partial digital protections only.	Maps all critical exchanges; defines engineering/operations-based verifications to prevent manipulation.

Appendix A – CIE Grant Rubric (Cont'd)

CIE Principle	Key Evaluation Question(s)	Scoring		
		1 Point – Needs Improvement	2 Points – Acceptable	3 Points – Exceptional
4. Design Simplification	▪ What unnecessary features can be removed or replaced with non-digital alternatives?	Minimum functionality unclear; no simplification measures.	Some unneeded features identified; limited alternatives.	Fully defines minimal functional set; removes or monitors excess features; adds non-digital redundancy.
5. Layered Defense	▪ What digital and engineered defense layers exist? ▪ Are they independent?	Layers not tied to consequence prevention.	Digital layers defined; limited independence or redundancy.	Diverse, redundant, independent digital + engineered layers preventing single-point failure.
6. Active Defense	▪ What indicators or precursors reveal a high-consequence event? ▪ How are operators trained to respond?	No indicators or response strategy; shifts risk to end user.	Defines some indicators or digital-only actions; limited training.	Documented strategies combining digital and manual responses; trained staff and exercises in place.
7. Interdependence Evaluation	▪ What external dependencies exist? ▪ How will critical functions continue if they fail?	Dependencies unrecognized; no alternatives.	Some dependencies described; limited backup options.	Fully identifies dependencies; defines redundant sources or fallback operations.

Appendix A – CIE Grant Rubric (Cont'd)

CIE Principle	Key Evaluation Question(s)	Scoring		
		1 Point – Needs Improvement	2 Points – Acceptable	3 Points – Exceptional
8. Digital Asset Awareness	▪ How are asset changes tracked and defended when patching is limited?	No asset tracking; fragmented systems.	Manual or partial tracking; disjointed IT/OT systems.	Centralized, mostly automated tracking; covers OT and IT; includes alternative defenses when patching deferred.
9. Cyber Secure Supply Chain	▪ How does the design mitigate supply-chain risks and ensure continuity?	Unproven suppliers; no continuity planning.	Familiar tech with partial continuity measures.	Proven suppliers; multi-source or alternate delivery; extended warranties; validated integrity checks.
10. Planned Resilience	▪ How will systems maintain safety and operation under partial or total automation loss?	No fail-safe design; no manual operation plan.	Partial documentation; unverified manual modes.	Verified fail-safe / fail-secure designs; tested manual operation for full functionality.

Appendix A – CIE Grant Rubric (Cont'd)

CIE Principle	Key Evaluation Question(s)	Scoring		
		1 Point – Needs Improvement	2 Points – Acceptable	3 Points – Exceptional
11. Engineered Information Control	▪ What sensitive engineering info is protected, and how is access controlled?	Info widely available; no controls.	Some restrictions; partial contract enforcement.	Controlled access; formal NDAs/data-handling clauses; verified protections for diagrams/configurations.
12. Organizational Culture	▪ What training and procedures ensure safe, secure, informed operation and maintenance?	Dangerous assumptions about skills; no training.	Some training; limited continuity or alternatives.	Defined expertise levels; continuous training or subcontracted support; operators consider cyber sabotage in diagnostics.

Section 3 – Appendix B

Impact Scorecards

Appendix B - Impact Scorecards in Practice

A standardized consequence framework for evaluating cybersecurity and data-integrity events through an engineering lens.

Purpose: Provide a consistent, 1–5 scale for assessing cyber and data-integrity impacts.

Scope: Applies across health & safety, asset damage, financial loss, environmental, and public confidence categories.

Principle: Grounded in engineering ethics for public safety first.

Score	Impact Level	Description
1	Insignificant	Minor disruption of non-critical IT/OT systems; quickly contained.
2	Minor	Temporary loss of some digital functions; limited manual workarounds available.
3	Moderate	Manipulation or outage of control/data flows affecting reliability; requires extended recovery.
4	Significant	Compromise of critical OT data or systems; major operational disruption, safety margins stressed.
5	Severe	Catastrophic cyber compromise; loss of control or trust in automation leading to prolonged outages or cascading failures.

Section 3 – Appendix C

Future Additional Use Cases

CIE Toolkit for Regulators (in partnership with NARUC)

INL and NARUC can collaborate to create a toolkit that embeds cyber-informed engineering into state regulatory and engineering review.

- Provides regulators and PUC engineers with step-by-step CIE methods for evaluating digital projects
- Includes checklists, scenarios, and training modules for grid-modernization cases
- Aligns with state oversight responsibilities for cybersecurity, reliability, and safety
- Builds regulator capacity to review CIE-based grant proposals, interconnection filings, and vendor claims
- Promotes a consistent national approach to cyber-engineering governance

CIE for Virtual Power Plantsand Mass Control Architectures

CIE principles strengthen DER systems by addressing cybersecurity and dependency risks across large, coordinated resource networks.

- Applies CIE to VPP aggregation platforms and distributed control layers
- Identifies and mitigates risks in communication links, dispatch algorithms, and automation logic
- Supports secure coordination of DERs, storage, and responsive load resources
- Enables consequence-based design for system resilience under cyber or control failures
- Informs state or utility standards for secure VPP deployment and operation

CIE for Capacity Analysis and Long-Term Planning

Integrating CIE into capacity studies allows states to pair traditional reliability metrics with assessments of cyber-driven vulnerabilities.

- Embeds cyber-risk factors into capacity-planning and adequacy models
- Evaluates how digital dependencies (controls, sensors, data systems) affect reserve margins and response time
- Enables scenario modeling for cyber disruptions and cascading operational impacts
- Guides investment toward secure, resilient generation and grid capacity portfolios
- Positions CIE as a planning discipline within resource-adequacy and infrastructure-resilience frameworks

Section 4 – Appendix D: Other Use Cases

Qualitive Criteria for State Funded Grants

Integrating Quantitative Criteria

Quantitative criteria are included in RFPs as measurable thresholds for safety, performance, and reliability.

What is it: Measurable thresholds for safety, performance, and reliability (e.g., voltage, load served, recovery times).

Example: “Safety: Voltage < 240V; Performance: ≥ 80% load served for 7 days; Reliability: MTTR ≤ 48 hrs.”

1. **Efficiency Metrics:** Define performance and recovery expectations (e.g., mean time to repair, system capacity).
2. **Safety Thresholds:** Set operating limits and require safeguards (e.g., voltage/frequency bounds, mechanical interlocks).
3. **Reliability Targets:** Establish failure rates and durability standards (e.g., mean time between failures, acceptable failure frequency).

Quantitative criteria turn resilience into engineering specifications. They ensure proposals can be tested against clear, measurable thresholds.

Section 4 - Appendix E: Other Use Cases

Risk Assessments and INL Assistance

How INL Assists States with Cyber-Informed Risk and Resilience

INL provides states with the technical expertise and engineering frameworks needed to identify, manage, and mitigate cyber-physical risks.

- Delivers **training and technical assistance** on CIE methods and tools
- Guides **policy and technical coordination** for BESS, microgrids, and DERs
- **Develops mitigations**: secure comms, segmentation, and supply-chain assurance
- Enhances coordination among **state agencies, utilities, and integrators**
- Provides **specialized tools and templates**:
  - CIEBAT / CIEMAT for system risk analysis
  - BESSE kits for inspection and configuration
  - State reference designs and allow-lists

What is CIEBAT?

- **Evaluates** comms loss, control compromise, and timing drift
- **Recommends layered mitigations** such as redundant control paths and authenticated comms

CIE in Risk Assessments: Identifying and Prioritizing Digital Risk

By applying risk-assessment frameworks, INL helps decision-makers focus on the digital functions that create the consequences.

- Strengthens **state resiliency planning** through digital-risk evaluation
- Identifies **high-consequence components and functions**
- Treats **"digital functions" as risk factors** (control logic, timing, data integrity)
- **Reprioritizes mitigations** toward high-impact vulnerabilities

BESS & Microgrid Examples:

- **Evaluates** comms loss, control compromise, and timing drift
- **Recommends layered mitigations** such as redundant control paths and authenticated comms

CIE for Interconnection Risk Mitigation

CIE enables states to strengthen interconnection reviews by adding cybersecurity-driven and digital risk analysis to DER and IBR integration.

Cybersecurity challenge:

- **Limited Digital Risk Mitigation** (IEEE 1547.3 – DER Cybersecurity interconnection standard focuses on information security, not functional resilience)
- DERs and IBRs **introduce new attack surfaces** that can affect grid stability

INL assists states by integrating CIE into interconnection analysis:

- **Simulates worst-case** operational scenarios
- **Uses CIE questions** to identify and "engineer out" high-consequence events
- **Documents required mitigations** in state supplemental reports

Adds **cyber-resilience criteria** to state approval and certification processes

Bills of Materials (BOMs) for Supply-Chain Assurance

BOMs improve visibility into component origins and dependencies, advancing secure procurement and maintenance.

Current Issues:

- Inconsistent formats
- False positives
- Sharing constraints

INL assists states by:

- Defining “good” / actionable BOMs
- Building trusted data-sharing frameworks
- Exploring automation and data-standard alignment

Positions BOMs as a core supply-chain security tool within CIE

Section 4 - Appendix F: Other Use Cases

Day Without Automation

“Day Without Automation”: The Concept

This exercise imagines a grid operating for one day with no digital controls, sensors, or automation and asks: what still works and what fails?

Normal State: Automated Operations

Event: Automation Failure

Response: Manual Recovery & Local Control

Exercise Outcomes:

- Simulates a total loss of automation to expose hidden dependencies
- Identifies critical manual functions needed for safe, stable operation
- Reveals design gaps in fallback control, communication, and local logic
- Drives engineering mitigations: isolation, manual overrides, local autonomy

How States Deploy This Exercise

This exercise is a practical tool for evaluating grant applications, reviewing interconnection requests, and training utilities on automation dependencies.

Format and Facilitation

- **Workshop/Tabletop Exercise**: States facilitate this as a structured discussion or tabletop exercise with utility partners
- **Participants**: State energy office staff, utility engineers, and project developers

When to Deploy

- **Grant evaluation**: Require applicants to document automation dependencies and manual operation capabilities
- **Interconnection review**: Assess DER/microgrid proposals for failsafe design and degraded-mode operations
- **Utility partnerships**: Host workshops to build CIE awareness and identify shared infrastructure risks

How to Conduct a “Day without Automation” Review

States and utilities can follow this four-step process to systematically identify automation dependencies and engineer resilient safeguards.

Define

Map automation dependencies and essential digital functions

Simulate

Remove automation from the scenario for 24 hours

Assess

Identify what fails, what can continue, and what’s missing

Engineer

Add safeguards: manual operations, segmentation, local autonomy

Applies to BESS, Microgrids, VPPs, and interconnection processes to reveal hidden risks and strengthen design.

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.