INL/MIS-23-71048-Revision-0

Cyber-Informed Engineering

January 2023

Virginia L Wright

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-23-71048-Revision-0

Cyber-Informed Engineering

Virginia L Wright

January 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Cyber-Informed Engineering

INL is managed by Battelle Energy Alliance
for the US Department of Energy

Idaho National Laboratory

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 engender a **culture of security** aligned with the existing industry safety culture.

CIE and Technology Readiness Levels

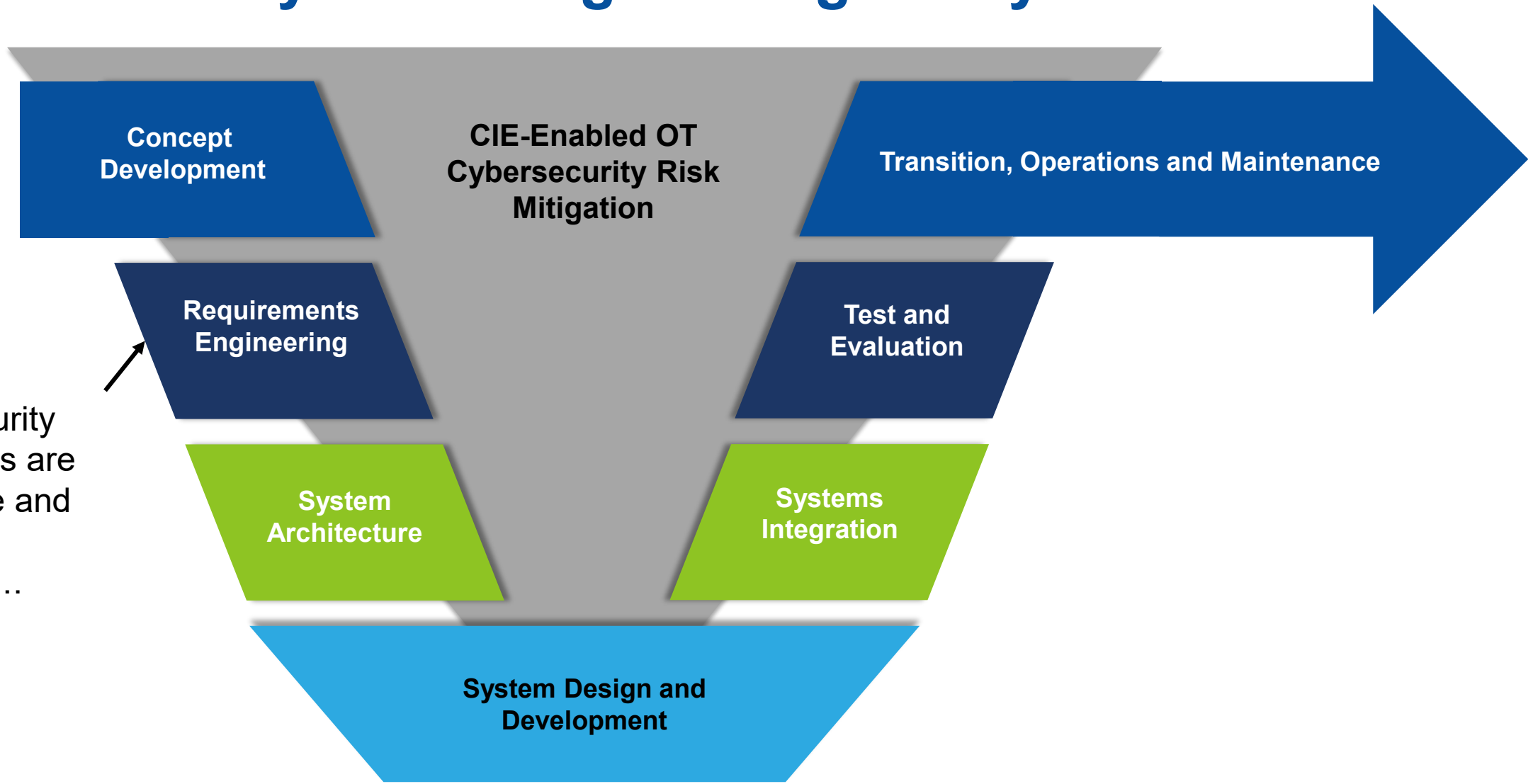
Traditional OT Cybersecurity risk mitigations are usually applied here…

CIE and Technology Readiness Levels

Traditional OT Cybersecurity risk mitigations are usually applied here…

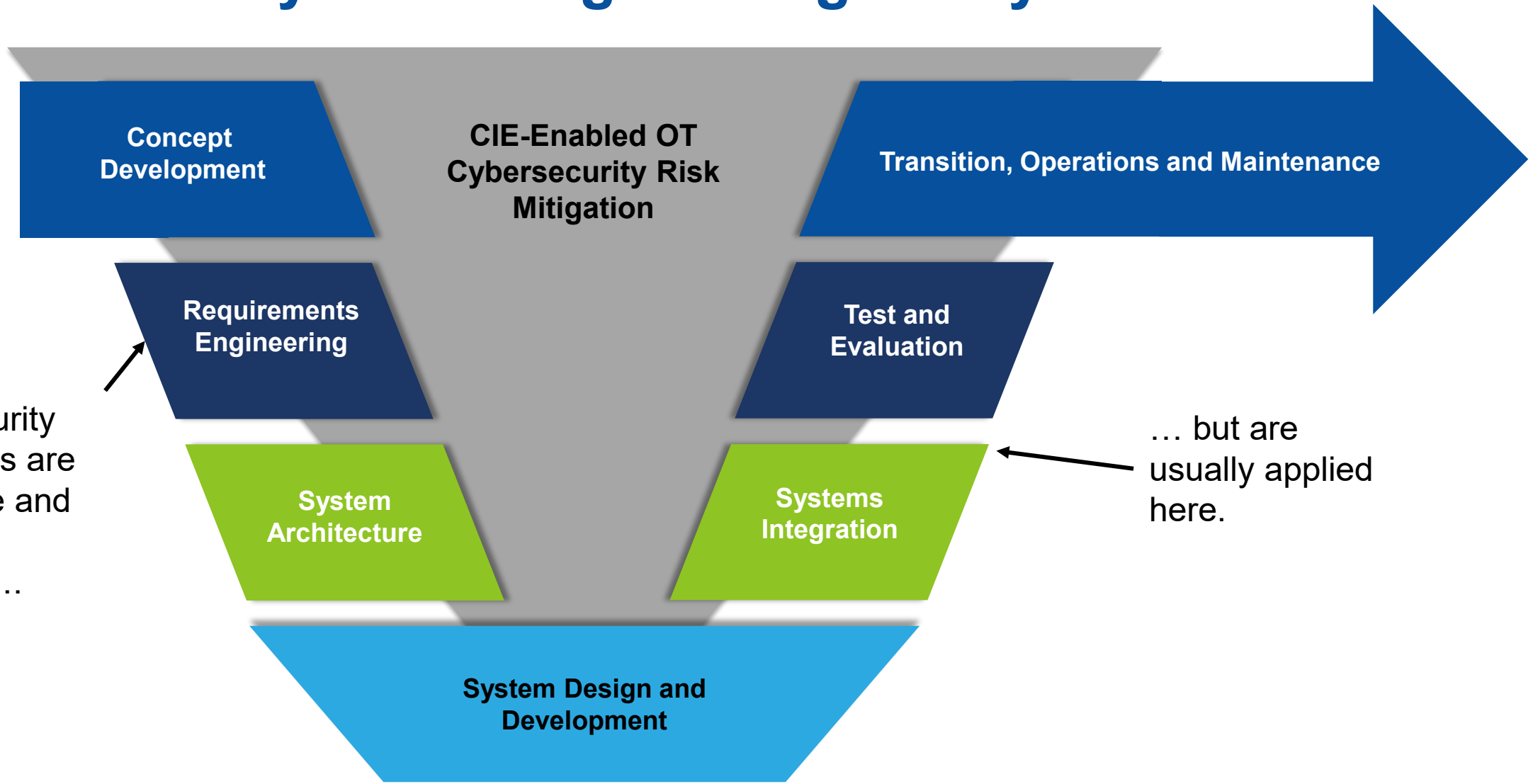
… but are more effective and efficient when applied here.

CIE and the Systems Engineering Lifecycle



OT Cybersecurity risk mitigations are more effective and efficient when applied here….

CIE and the Systems Engineering Lifecycle



OT Cybersecurity risk mitigations are more effective and efficient when applied here….

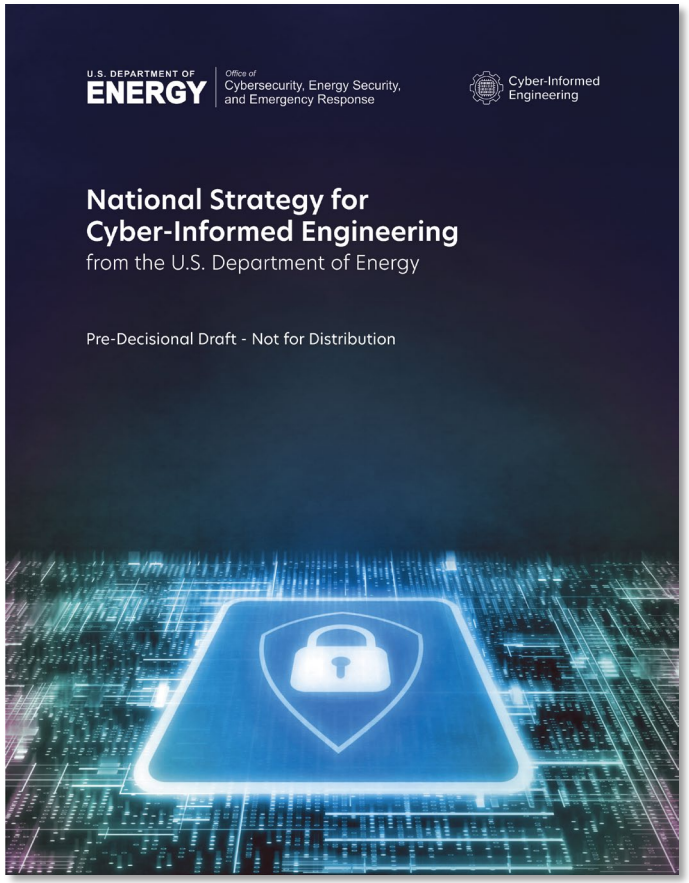
… but are usually applied here.

Principles of CIE

DESIGN AND OPERATIONS	ORGANIZATIONAL
Consequence-focused design	Interdependency evaluation
Engineered controls	Digital asset awareness
Secure information architecture	Cyber-secure supply chain controls
Design simplification	Planned resilience
Resilient layered defenses	Engineering information control
Active defense	Cybersecurity culture

National CIE Strategy

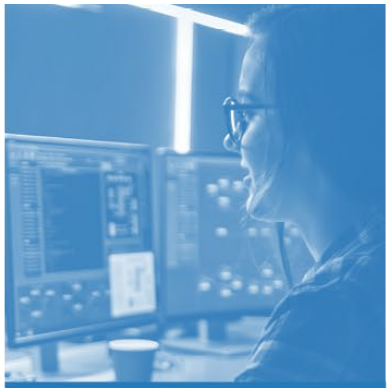
- Directed by the U.S. Congress in the Fiscal Year 2020 National Defense Authorization Act
- Outlines core CIE concepts
  - Defined by a set of design, operational, and organizational principles
  - Place cybersecurity considerations at the foundation of control systems design and engineering
- Five integrated pillars offer recommendations to incorporate CIE as a common practice for control systems engineers
  - Intended to drive action across the industrial base stakeholders—government, owners and operators, manufacturers, researchers, academia, and training and standards organizations
- DOE issued the National CIE Strategy June 15, 2022



Pillars of the National CIE Strategy

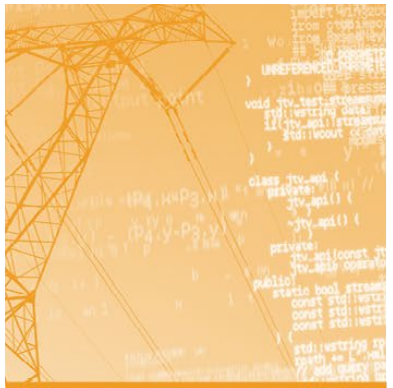
Awareness

Promulgate a universal and shared understanding of CIE



Education

Embed CIE into formal education, training, and credentialing



Development

Build the body of knowledge by which CIE is applied to specific implementations

Current Infrastructure

Apply CIE principles to existing systemically important critical infrastructure

Future Infrastructure

Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology

National CIE Strategy Pillar: Awareness

Awareness

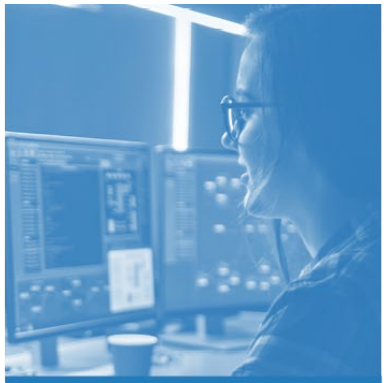
Promulgate a universal and shared understanding of CIE

Raise awareness of the CIE approach, gaps it addresses, CIE's application potential, and major benefits among decision makers in the engineering community.

STRATEGIC RECOMMENDATIONS

- Lead a CIE awareness campaign to support a shift in the culture of energy infrastructure engineering and operations.
- Formulate the technical requirements to implement CIE principles.
- Develop policy initiatives and build partnerships to incentivize the broad adoption of CIE in the energy industry.
- Develop and promote case studies that demonstrate the benefits of applying CIE to existing and emerging infrastructure systems.

National CIE Strategy Pillars



Education

Embed CIE into formal education, training, and credentialing

Develop a pipeline of CIE practitioners through education, training, and certification of CIE knowledge and skills.

STRATEGIC RECOMMENDATIONS

- Create near-term CIE training and credentialing programs to rapidly produce a CIE-savvy workforce available to secure energy infrastructure.
- Partner with academia to embed CIE principles into appropriate courses and degree programs at the undergraduate and graduate levels.
- Partner with industry employers to ensure alignment between CIE curricula and certifications, and demand signals from employers.
- Identify and partner with federal programs that support engineering and technical workforce education to include of CIE principles and enrichment.

National CIE Strategy Pillars

Development

Build the body of knowledge by which CIE is applied to specific implementations

Mature CIE approaches and promote broad application by building a repository of tools, practices, methods, and other enrichments to apply CIE to built and new infrastructure and validate CIE applications.

STRATEGIC RECOMMENDATIONS

- Leverage DOE's National Laboratories, academia, government partners, and industry to continually improve and expand the applicability of CIE.
- Create a CIE Center of Excellence to coordinate and drive the maturation of CIE.
- Create and maintain an open-source library of CIE tools, case studies, and lessons that support designers, manufactures, and asset owners and operators in applying CIE principles.

National CIE Strategy Pillars

Current Infrastructure

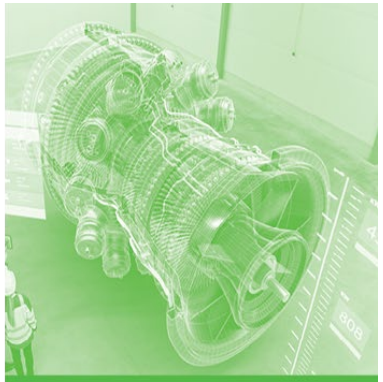
Apply CIE principles to existing systemically important critical infrastructure

Use a consequence-driven approach to identify and apply CIE principles to the nation's systemically important critical infrastructure already commissioned and in service today.

STRATEGIC RECOMMENDATIONS

- Prioritize current infrastructure to apply CIE principles and identify needed upgrades.
- Identify, document, and promote methods to apply CIE principles to reduce high-consequence impacts on existing infrastructure types that offer a high return on investment.
- Develop methods to assess and validate the effectiveness of infrastructure upgrades and mitigations identified through CIE.
- Embed CIE into procurement decisions and provide incentives to asset owners who invest in applying CIE principles to secure high-priority existing infrastructure.

National CIE Strategy Pillars



Future Infrastructure

Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology

Nurture and sustain an Energy Sector Industrial Base that enables manufacturers and asset owners to apply CIE principles into the full lifecycle of newly commissioned critical infrastructure systems.

STRATEGIC RECOMMENDATIONS

- Develop novel concepts for critical function assurance in emerging technologies that identify and revise design patterns that lead to high-consequence cyber-enabled impacts.
- Drive the creation or revision of International Standards for design, production, and lifecycle support capabilities to embody CIE principles.
- Provide market incentives that drive R&D and suppliers to apply CIE principles to their offerings as a long-term competitive advantage.
- Prioritize federal support to national, state, and local infrastructure system projects designed, built, and maintained using CIE standards and approaches.

Implementation Underway of National CIE Strategy

- DOE researchers are using CIE to ensure cybersecurity is at the forefront of advanced nuclear reactor technology design.
- EERE's Wind Energy Technology Office included CIE as a key recommendation for reducing cyber risk in the wind industry.
- The EERE-sponsored Cyber Manufacturing Innovation Institute (CyManII) included CIE implementation in its 2022 Research Roadmap and is supporting several public-private implementation projects for the advanced manufacturing community.
- A new Computer Systems Engineering Bachelor of Science degree program at Boise State University (BSU) is the first accredited engineering degree to incorporate INL's research in CIE.
- Auburn University committed to offering CIE classes in its engineering school
- The University of Texas, San Antonio, has committed to building a dedicated CIE Lab in 2023

Resources

- National Cyber-informed Engineering Strategy – https://bit.ly/3z2yI3F
- Cyber-Informed Engineering – www.inl.gov/cie
- Consequence-Driven, Cyber-Informed Engineering – www.inl.gov/cce
- To Join – CIE@inl.gov

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.