RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SAT-M02**

Be Debt Free!
Using Cyber-Informed Engineering to Future-Proof Technology

Cheri Caddy

Senior Advisor for Cybersecurity
U.S. Department of Energy
Office of Cybersecurity, Energy Security, and Emergency Response

Steven Kunsman

Director Product Management and Applications
Hitachi Energy

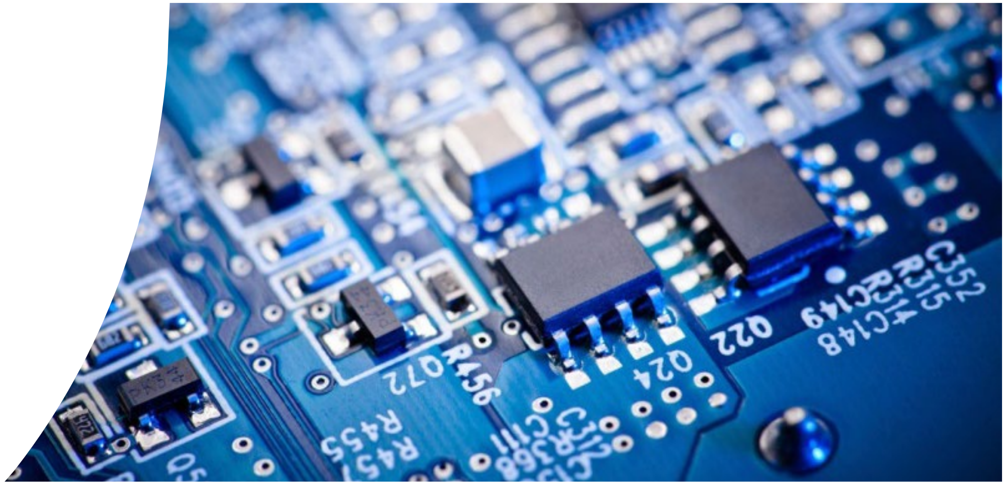
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

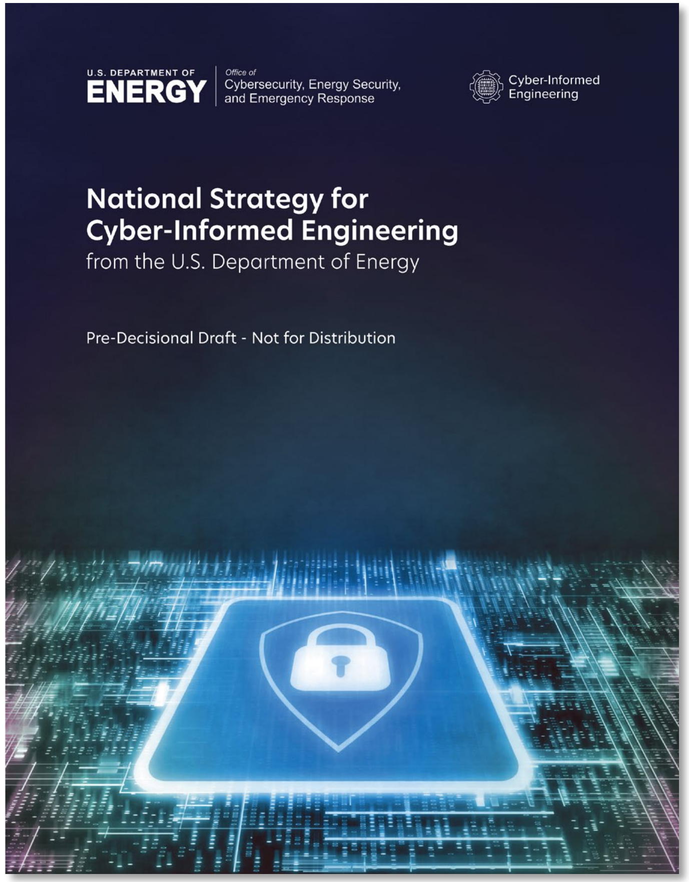
Cyber-Informed Engineering (CIE)

- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to "engineer out" cyber risk** 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.



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 is issuing the National CIE Strategy in June 2022



U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Cyber-Informed Engineering

National Strategy for Cyber-Informed Engineering

from the U.S. Department of Energy

Pre-Decisional Draft - Not for Distribution

Principles of CIE

Design and Operational Principles	**Organizational Principles**
Consequence-focused design	Interdependency evaluation
Engineered controls	Digital asset awareness
Secure information architecture	Cyber-secure supply chain controls
Design simplification	Planned resilience with no assumed security
Resilient layered defenses	Engineering information control
Active defense	Cybersecurity culture

Key Premises of the CIE Strategy

Today's risk landscape calls for systems that are engineered to continue operating critical functions while faced with increasingly severe and sophisticated cyber attacks from intelligent, determined adversaries.

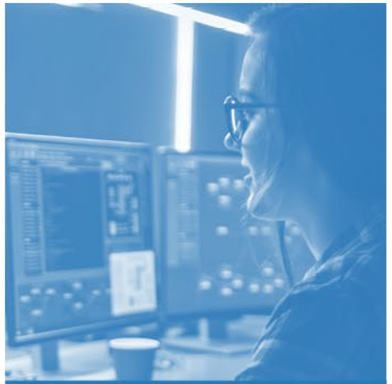
While specialized IT and OT cybersecurity experts bring strong skills, **many engineers and technicians who design and operate control systems with digital components currently lack sufficient cybersecurity education** and training to adequately address the risk of cyber-enabled sabotage, exploitation, failure, and misuse in the design, development, and operational lifecycle.

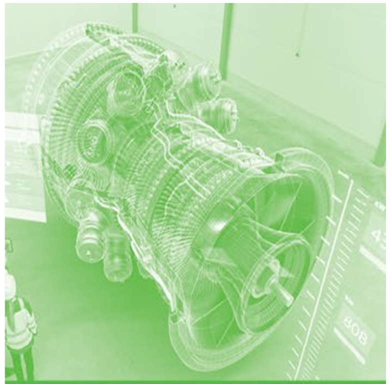
Accelerating industry's adoption of a culture of cybersecurity by design—complementing industry's strong culture of safety—offers the ability to maintain secure design even as systems evolve and grow in functionality.

CIE offers an opportunity to reduce risk across the entire device or system lifecycle, starting from the earliest possible phase of design.

Early in the design phase is often the most optimal time to achieve low cost and effective cybersecurity, compared to solutions introduced late in the engineering lifecycle.

Pillars of the Proposed National CIE Strategy





Awareness	Education	Development	Current Infrastructure	Future Infrastructure
Promulgate a universal and shared understanding of CIE	Embed CIE into formal education, training, and credentialing	Build the body of knowledge by which CIE is applied to specific implementations	Apply CIE principles to existing systemically important critical 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

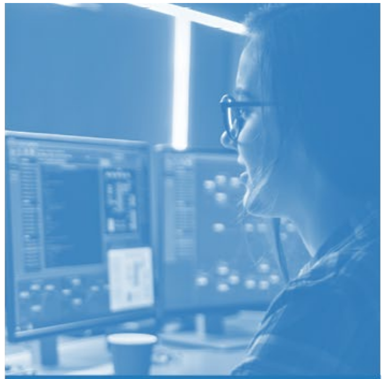
Promulgate a universal and shared understanding of CIE

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

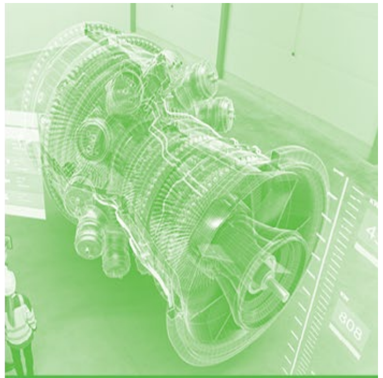
Apply CIE principles to existing systemically important critical infrastructure

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.

A Model
for Other Critical Infrastructure Sectors

- **CIE represents foundational engineering principles that have broad applicability** to engineers and industrial control systems across many critical infrastructure sectors
- **The National CIE Strategy can serve as a guide** for other critical infrastructure sectors to adopt and incorporate CIE into government and industry practices
- **Interdependencies among critical functions create an equal imperative** to incorporate CIE into energy and other critical infrastructure systems

National CIE Implementation Underway

- Stakeholders are already taking steps to move the strategy forward:
  - **Universities – integrating CIE concepts into engineering curriculum** at Boise State, Auburn, and UTSA
    - Boise State University offering a 1-credit CIE course in summer 2022
  - **Design Teams – exercising CIE concepts in the design/build** of groundbreaking portable nuclear microreactors for the U.S. Department of Defense
  - **Federal Agencies – scaling up Consequence-driven Cyber-informed Engineering (CCE)**, a methodology for implementing CIE concepts in organizations critical to national security
  - **Workforce – DoD added the Control System Security Specialist role within the Defense Cybersecurity Workforce,** elevating the importance of operational technology cybersecurity for workforce development

Apply What You Have Learned Today

- In the next month you should:
  - Read the National Cyber-Informed Engineering Strategy
  - Send us feedback or express interest: cie@inl.gov
- In the next three months you should:
  - Examine your organization's operations through the lens of the CIE principles and identify gaps
  - Identify actions/efforts in the strategy where your organization could participate to implement Cyber-Informed Engineering
- In the next six months you should:
  - Look for announcements on opportunities to engage in community-wide implementation efforts organized around the five pillars of the CIE Strategy