Cyber-Informed
Engineering

Cyber-Informed Engineering

Virginia Wright
INL Idaho National Laboratory

INL Background

- One in a network of 17 DOE national labs
- DOE’s lead lab for nuclear energy
- A major center for National Security

5,690 Employees | 511 Interns | $1.5 B Budget | 255 Patents

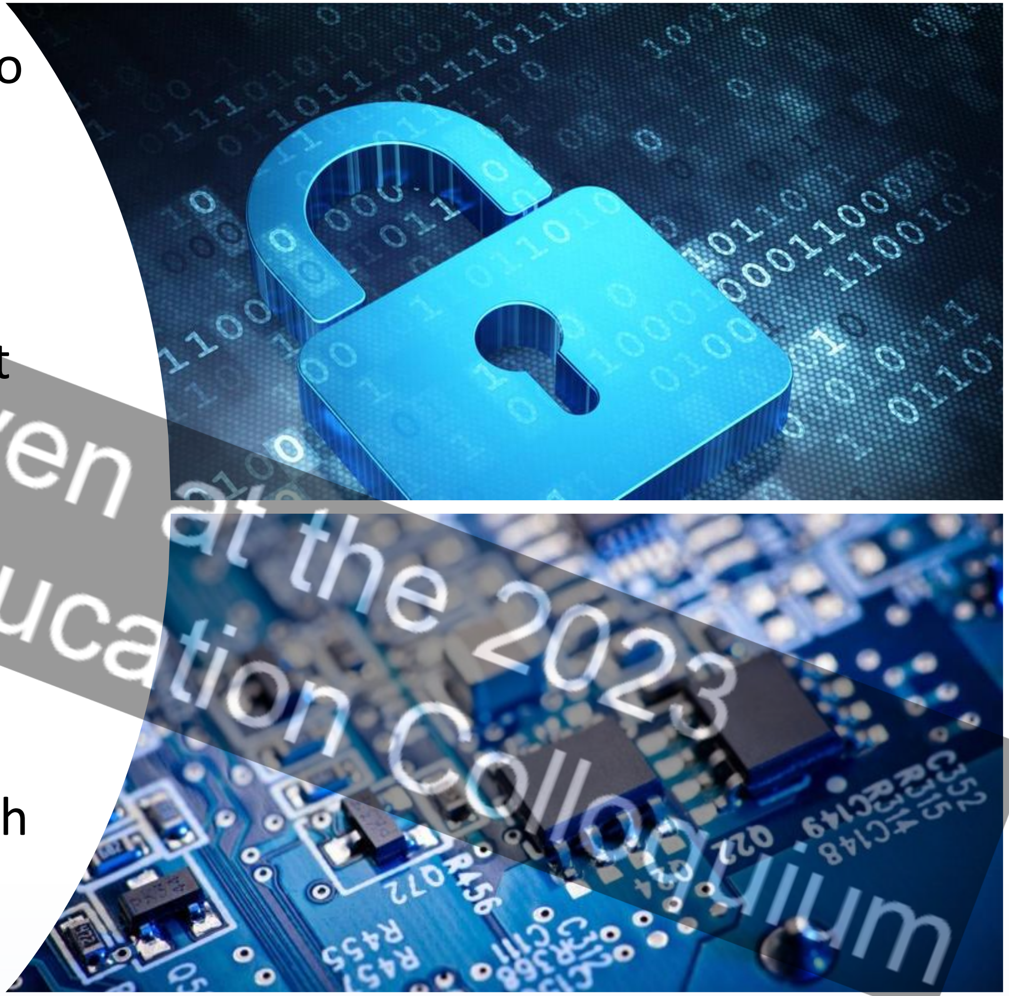
INL Mission
Our mission is to discover, demonstrate and secure innovative nuclear energy solutions, other clean energy options and critical infrastructure.

INL Vision
INL will change the world’s energy future and secure our critical infrastructure.

Research in the National Interest that **Maintains American Competitiveness & Security**

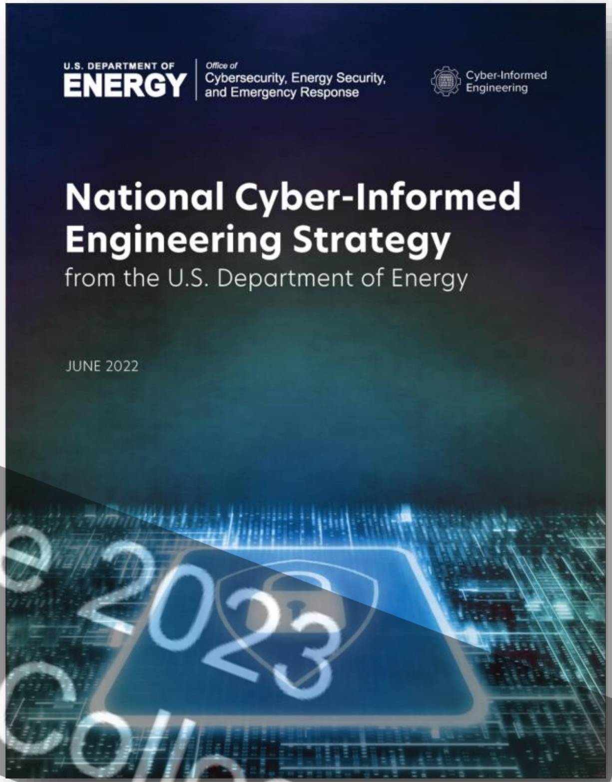
Cyber-Informed Engineering (CIE)

- 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.



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
  - Placed 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	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

CIE Principles

Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary?
Resilient Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

CIE COP and Working Group Purpose

Cyber-Informed Engineering COP

Quarterly

11 AM ET on the 2nd Wednesday of January, April, July, and October

Multi-stakeholder team to aid the translation of CIE into technical requirements that can inform guidance, practices, and standards development

Working Group	Purpose
CIE Standards WG Monthly 1st Wednesday, 9 AM MT / 11 AM ET	Support integration of CIE into engineering and cybersecurity standards
CIE Education WG Monthly 3rd Wednesday, 9 AM MT / 11 AM ET	Develop curricula and materials that integrate CIE principles into engineering degree programs
CIE Development WG Monthly 4th Wednesday, 9 AM MT / 11 AM ET	Develop CIE implementation guidance and an open-source library of resources

CIE Open-Source Library

Title	Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs for Phase 2 of the Secure Power Systems Professional project
Authors	O'Neil, Lori Ross; Assante, Michael; Tobey, D. H.; Conway, T. J.; Vanderhorst, Jr, T. J.; Januszewski, III, J.; leo, R.; Perman, K.
Description	This is the final report of Phase 2 of the Secure Power Systems Professional project, a 3 phase project. DOE will post to their website upon release.
Authoring Organization	Pacific Northwest National Lab. (PNNL), Richland, WA (United States)
Sponsoring Organization	USDOE
Metadata	Metadata
Full Document	Full Document

Title	Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology
Authors	Price, Joseph Daniel; Anderson, Robert Stephen
Description	Current engineering and risk management methodologies do not contain the foundational assumptions required to address the intelligent adversary's capabilities in malevolent cyber attacks. Current methodologies focus on equipment failures or human error as initiating events for a hazard, while cyber attacks use the functionality of a trusted system to perform operations outside of the intended design and without the operator's knowledge. These threats can by-pass or manipulate traditionally engineered safety barriers and present false information, invalidating the fundamental basis of a safety analysis. Cyber threats must be fundamentally analyzed from a completely new perspective where neither equipment nor human operation can be fully trusted. A new risk analysis and design methodology needs to be developed to address this rapidly evolving threatscape.
Authoring Organization	Idaho National Lab. (INL), Idaho Falls, ID (United States)
Sponsoring Organization	USDOE National Nuclear Security Administration (NNSA)
Metadata	Metadata
Full Document	Full Document

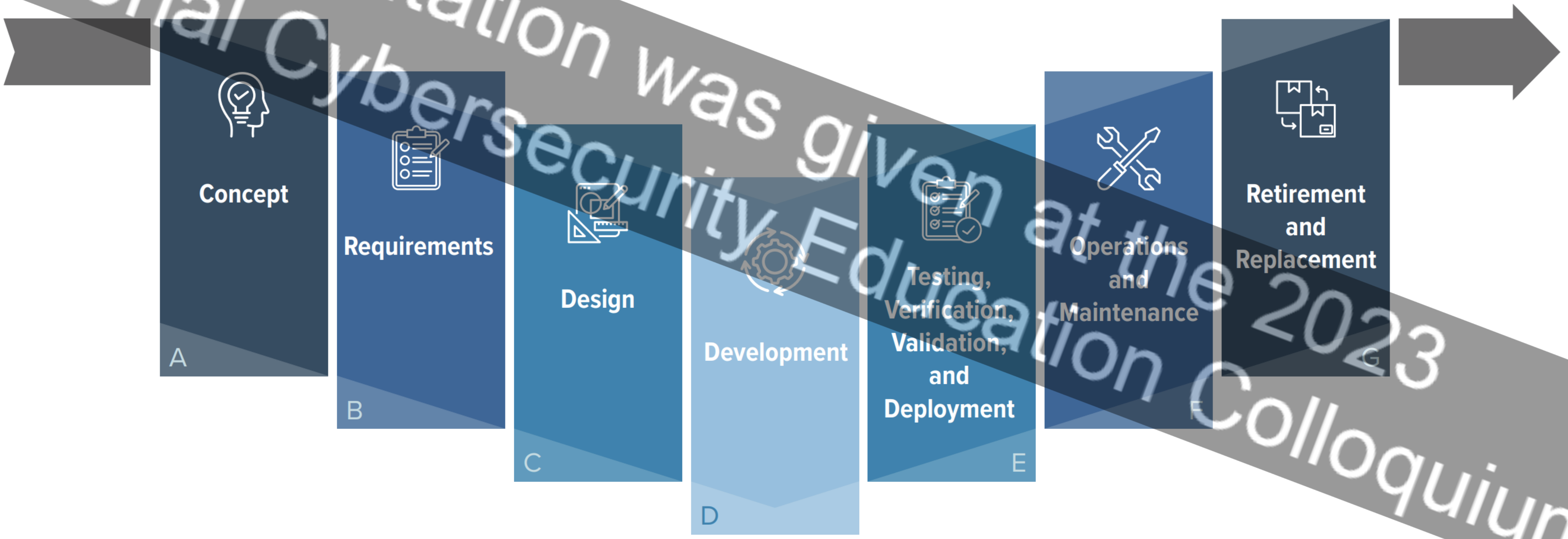
Title	Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector
Authors	Glenn, Colleen; Sterbentz, Dane; Wright, Aaron
Description	With utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyber attacks on the North American electric grid continue to grow in frequency and sophistication. The potential for malicious actors to access and adversely affect physical electricity assets of U.S. electricity generation, transmission, or distribution systems via cyber means is a primary concern for utilities contributing to the bulk electric system. This paper seeks to illustrate the current cyber-physical landscape of the U.S. electric sector in the context of its vulnerabilities to cyber attacks, the likelihood of cyber attacks, and the impacts cyber events and threat actors can achieve on the power grid. In addition, this paper highlights utility perspectives, perceived challenges, and requests for assistance in addressing cyber threats to the electric sector. There have been no reported targeted cyber attacks carried out against utilities in the U.S. that have resulted in permanent or long term damage to power system operations thus far, yet electric utilities throughout the U.S. have seen a steady rise in cyber and physical security related events that continue to raise concern. Asset owners and operators understand that the effects of a coordinated cyber and physical attack on a utility's operations would threaten electric system reliability–and potentially result in large scale power outages. Utilities are routinely faced with new challenges for dealing with these cyber threats to the grid and consequently maintain a set of best practices to keep systems secure and up to date. Among the greatest challenges is a lack of knowledge or strategy to mitigate new risks that emerge as a result of an exponential rise in complexity of modern control systems. This paper compiles an open-source analysis of cyber threats and risks to the electric grid, utility best practices for prevention and response to cyber threats, and utility suggestions about how the federal government can aid utilities in combating and mitigating risks.
Authoring Organization	Idaho National Lab. (INL), Idaho Falls, ID (United States)
Sponsoring Organization	USDOE Office of Energy Policy and Systems Analysis (EPSA)
Metadata	Metadata

- DOE-sponsored research on Cyber-Informed Engineering as far back as 2013
- Multiple laboratories
- Multiple Application Areas

CIE Implementation Guide

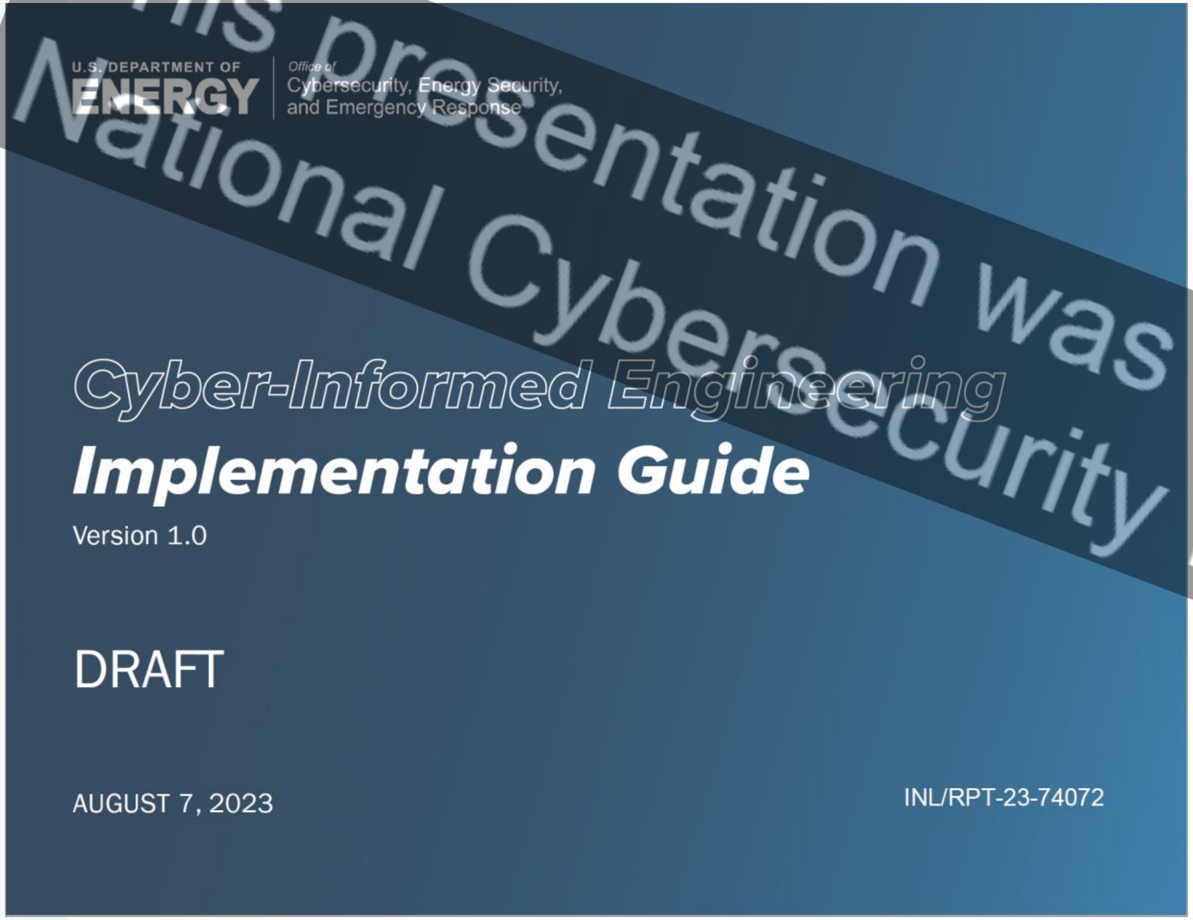
Applying CIE across the SE Lifecycle

Figure 2. CIE Systems Engineering Lifecycle Model



Cyber-Informed Engineering

CIE Implementation Guide


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

Cyber-Informed Engineering

Implementation Guide

Version 1.0

DRAFT

AUGUST 7, 2023

INL/RPT-23-74072

https://www.osti.gov/servlets/purl/1995796

CIE Implementation Guide

U.S. DEPARTMENT OF ENERGY

Cyber-I...

Implem...

Version 1.0

DRAFT

AUGUST 7, 2023

PRINCIPLE 1

Consequence-Focused Design

1

KEY QUESTION

How do I understand what critical functions my system must <u>ensure</u> and the undesired consequences it must <u>prevent</u>?

Principle Description

Apply CIE strategies first and foremost to the most critical functions the system performs. Typically these are functions that, if manipulated or subverted, could result in unacceptable or catastrophic consequences for the organization, including undesired impacts to security, safety, quality, the environment, availability or effectiveness of products or services, system integrity, and public image. Use a structured and thorough process to identify areas where digital technology is used within these functions.

Consider where an unprotected action or failure of the function that leverages digital technology might lead to a high-consequence event. These could include unauthorized system actions, invalid data that would drive an automated action, or interdiction of a digitally governed control. Examine the controls that exist to minimize impacts of misuse or failure and whether those controls are implemented via digital technology, physical mechanisms, or a combination of both.

This list of high-impact consequences underpins the work engineers will perform throughout the system design lifecycle and the actions to be taken and their priority within each CIE principle. For each element identified in the work above, engineers will consider engineered controls (see Principle 2: Engineered Controls), that could either remove the possibility for the unprotected action or mitigate its consequences. These changes complement traditional cybersecurity protections to increase the overall resilience of the system to undesired digital events that could result in catastrophic consequences.

Consequence-Focused Design Considerations at Each Lifecycle Phase

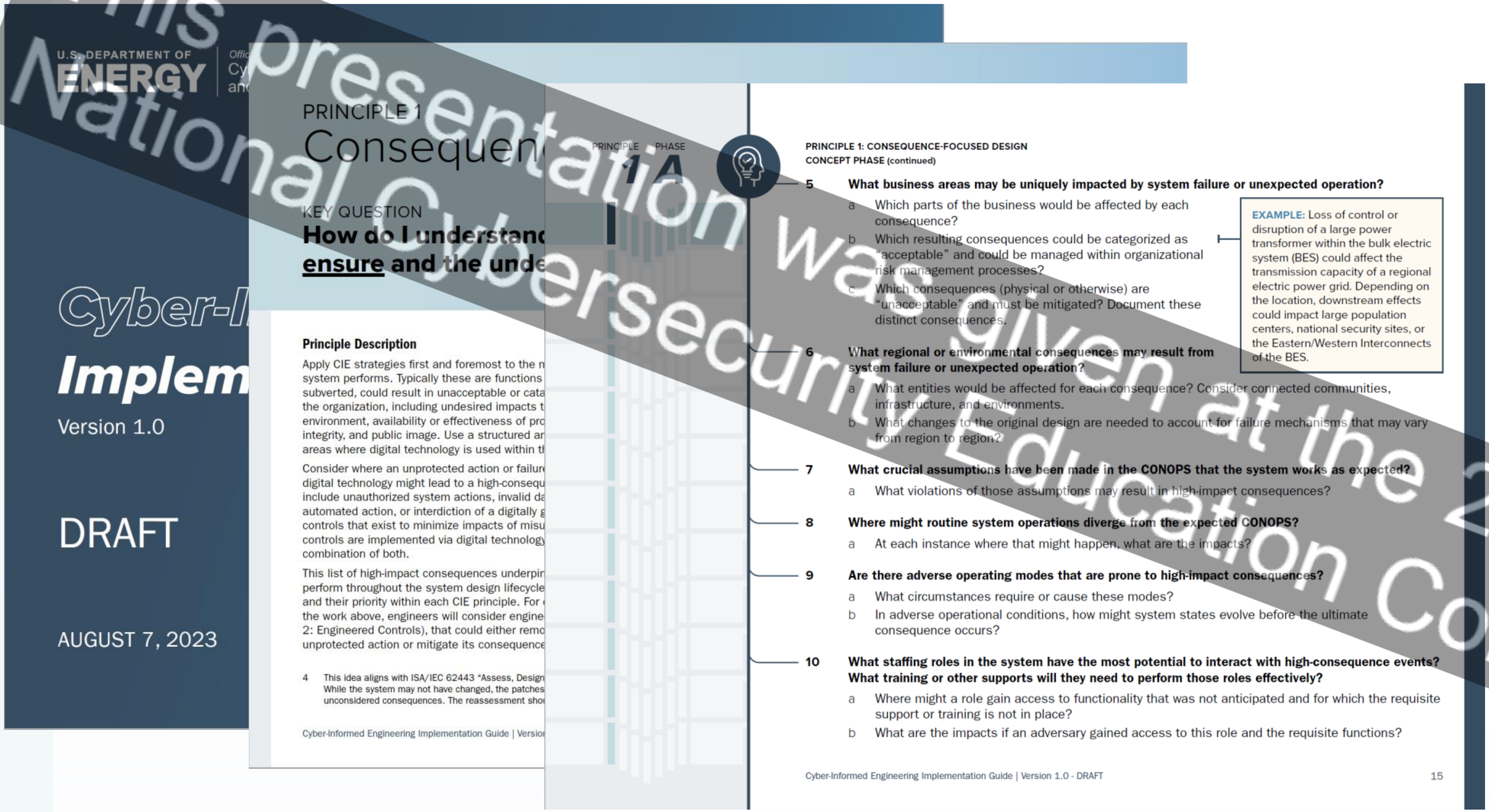
Because the Consequence-Focused Design principle provides key inputs for other principles, it should be the first principle considered at the beginning of the lifecycle phase. Consequence-Focused Design functions as a foundational principle that, once assessed, is used as the basis of consideration for all other principles. At a high level, early considerations may focus on identifying negative business consequences such as delivery failure, equipment damage, or impacts to safety, that may apply to the system generally, before linking consequences to specific design elements to engineered mitigations. Systems with a high potential for accidents, misuse, or sabotage resulting in catastrophic consequences will require a stronger emphasis on consequence-focused design.

Specific elements considered in the Consequence-Focused Design principle will shift as the principle is applied across time and system maturity. It is important to note that the trajectory of industry and technology changes may affect consequence assessment throughout a system's lifecycle. Consequence is a moving target that should be regularly re-assessed even if the considered system is not changing.[4]

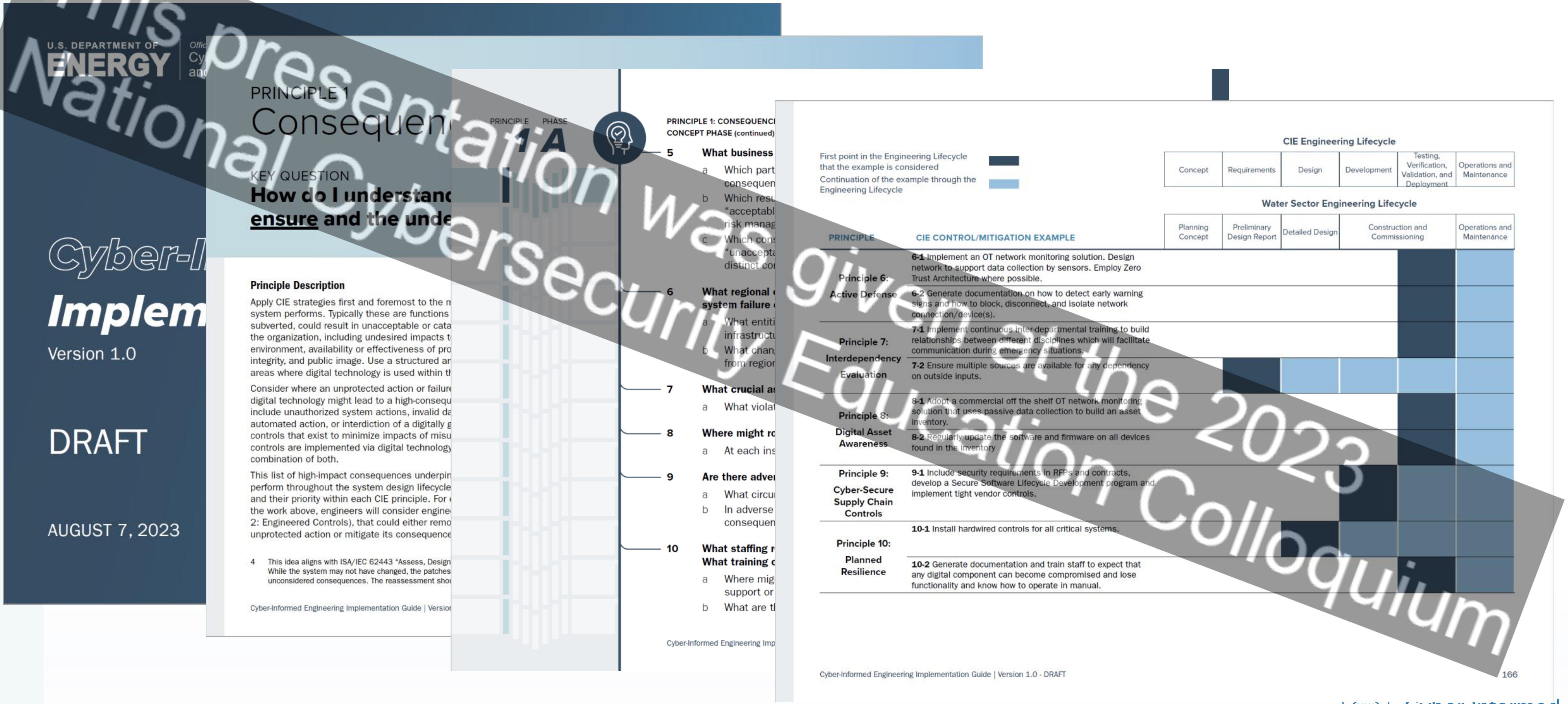
4 This idea aligns with ISA/IEC 62443 "Assess, Design & Implement, Operate & Maintain" 62443-3-2, which focuses on regular risk assessment for the System under Consideration (SuC). While the system may not have changed, the patches, updates, added users, third-party admin access to firewalls and switches, and organizational culture do often change, creating previously unconsidered consequences. The reassessment should also have externally vetted peer review to avoid internal company bias.

Cyber-Informed Engineering

CIE Implementation Guide



CIE Implementation Guide



Recent CIE Publications

Publications

- **CIE Implementation Guide:** Cyber-Informed Engineering Implementation Guide (Program Document) | OSTI.GOV
- **CIE Workbook:** https://www.osti.gov/biblio/1986517

Articles and Briefings

- **SANS ICS Concepts Video:** https://youtu.be/o_vIxW6UTeg
- **Industrial Cyber**: CIE and CCE Methodologies Can Deliver Engineered Industrial Systems for Holistic System Cybersecurity (June 11, 2023) with interviews from INL, 1898, and West Yost
- **Harvard Business Review:** Engineering Cybersecurity into U.S. Critical Infrastructure (April 17, 2023) by Ginger Wright, Andrew Ohrt, and Andy Bochman
- **Shift Left video podcast on GrammaTech blog:** Shifting Left for Energy Security (April 4, 2023) with Ginger Wright, Idaho National Lab and Marc Sachs, Auburn University
- For more CIE articles and publications, visit: inl.gov/cie

Next Steps

Working with Standards Bodies

- IEEE PES, and others
- ISA99 – 62443

Working with Universities

- Developing curriculum guidance
- Incorporating CIE into engineering education

Working with Asset Owners

- Incorporate CIE into ongoing efforts
- Refine products
- Procurement guidance, quantification of benefits

Thank You!

CIE@inl.gov
Virginia.Wright@inl.gov

https://www.linkedin.com/in/virginia-l-wright/

https://inl.gov/cie/

Idaho National Laboratory