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

Cyber-Informed Engineering

National Cyber-Informed Engineering Strategy

from the U.S. Department of Energy

JUNE 2022

Note from the Secretary

In today's increasingly interconnected world, America's safety and well-being depend on cybersecurity.

That's why President Biden considers hardening the nation against cyberattacks a top priority for his administration—and one that has only grown in importance as the country embarks on the biggest buildout of critical infrastructure and manufacturing capacity in a generation.

Each stage of the clean energy transformation that will bring with it an opportunity and an imperative to further increase security, reliability, and resilience in American's energy sector. The Cyber-Informed Engineering (CIE) Strategy shows us how we can seize the opportunity to address these challenges.

This framework, grown from earlier Congressional direction regarding threats to the nation's energy sector, advocates for an evolutionary shift across the energy industry and related institutions, including researchers, standards bodies, Federal partners, and others. Its recommendations reflect expertise and insight from energy companies, energy systems and cybersecurity manufacturers, standards bodies, researchers, DOE National Laboratories, and Federal partners in the cybersecurity and engineering mission space. It encourages the adoption of a "security-by-design" mindset within the Energy Sector Industrial Base, which refers to building cybersecurity into our energy systems at the earliest possible stages rather than trying to secure these critical systems after deployment. Thanks to President Biden's Bipartisan Infrastructure Law, we can match the CIE framework with new investments in clean energy infrastructure and manufacturing to begin building more secure clean energy systems here at home.

CIE further guides our cyber workforce development by helping us and our partners focus on the strategic intersection between cybersecurity and engineering, addressing gaps in how we train engineers and technicians and providing them with the means to build in security from the ground up. When our workforce is properly educated and supported, we are better positioned to manufacture and maintain the tools that help us prevent and quickly recover from cyberattacks.

This framework offers us a clear path forward to the future of energy security, in which America will stand at the forefront of global innovation and clean energy manufacturing. Following the CIE strategy will help ensure that our grid is not only resistant to initial attacks, but resilient enough to prevent and mitigate disruptions to our energy supplies, economy, and everyday lives.

I'd like to offer my deep gratitude and appreciation for the Securing Energy Infrastructure Executive Task Force (SEI ETF) who helped us take a critical step forward by leading the development of the CIE strategy. The work, however, continues. It will take close collaboration between government and industry to ensure energy systems of the future are designed and built for security and reliability. As we

pursue our transition to a completely clean energy sector, we will keep security and reliability front and center, and will need to stand shoulder-to-shoulder with our inter-agency partners at the Cybersecurity and Infrastructure Security Agency (CISA), National Institute for Standards and Technology (NIST), and more to ensure this CIE strategy is implemented to address current and future threat landscapes. Together, we will secure our energy sector and deliver a stronger, cleaner future.

Jennifer Granholm
Secretary
U.S. Department of Energy

Note from the Director

The U.S. energy sector faces ever-evolving cybersecurity threats. According to the 2022 Office of the Director of National Intelligence (DNI) Annual Threat Assessment[1], our adversaries maintain capabilities to launch cyberattacks that could disrupt critical infrastructure, including industrial control systems in the U.S. energy sector. Cybersecurity attacks on critical infrastructure are particularly consequential and ensuring the security, reliability, and resilience of these systems is a top priority for the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and its partners in government and the private sector.

This will take a concerted, collaborative effort between government and industry to ensure energy systems of the future are built securely to provide reliable energy to the nation. Building energy systems securely by design means ensuring all phases of the energy system life cycle – from design and development to installation and operation – are secure and can quickly recover from cyberattacks. The nation now has an unprecedented opportunity to shape the cybersecurity of our most critical infrastructure for decades to come.

The release of the Cyber-Informed Engineering (CIE) supports CESER's five priorities. Those priorities include: 1) Strengthening the visibility of cyber threats in energy systems; 2) Addressing supply chain risks; 3) Promoting security- and resilience-by-design; 4) Building cyber and resilience capacity in the private sector and the State, local, territorial, and tribal communities; and 5) Being prepared to respond in partnership with our government and industry partners when a cyber incident occurs in the energy sector. CIE, in many ways, cuts across all those priorities through its five pillars: awareness, education, development, current infrastructure, and future infrastructure.

CIE is an emerging framework, originated by the National Laboratories and advanced by DOE, to build cybersecurity into the nation's energy systems at the earliest possible stages rather than trying to secure these critical systems after deployment. CESER leads DOE's efforts to implement CIE to protect critical energy infrastructure assets and leverages expertise of its intra-agency partners. For example, CESER works closely with offices across the Department such as the Office of Energy Efficiency and Renewable Energy, the Office of Electricity, the Office of Intelligence and Counterintelligence, and others to ensure cybersecurity is built into energy systems of today and into the future.

As a power systems engineer, I know how critical it is to ensure that cybersecurity is built into standards used to design energy systems of the future. To that end, we will need partners with standards bodies such as the Institute of Electrical and Electronics Engineers (IEEE) and the International Electrotechnical

[1] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (April 2022), 4-24. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf.

Commission, educators and researchers in academia, and many others to help us champion the CIE principles. We need to ensure that cybersecurity is synonymous with reliability and safety in standards development working groups and in the hallways of engineering colleges to ensure we are successful. We can accomplish much more when we tackle these issues collaboratively.

Further, while DOE is leading this effort from an energy industry perspective, the overall approach will require close collaboration and significant work with its inter-agency partners at the Cybersecurity and Infrastructure Security Agency (CISA), National Institute for Standards and Technology (NIST), and others to ensure the CIE recommendations herein are implemented across the country to address the current and future threat landscapes.

I extend my thanks to the Securing Energy Infrastructure Executive Task Force and Idaho National Laboratory who were instrumental in the development of the strategy. The recommendations herein reflect the expertise of Energy Sector Industrial Base (ESIB) stakeholders comprised of energy companies, manufacturers, standards bodies, researchers, DOE National Laboratories, and Federal partners in the cybersecurity and engineering mission space.

Puesh Kumar
Director
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
U.S. Department of Energy

TABLE OF CONTENTS

Executive Summary

The Persistent Cybersecurity Challenge

The industrial control systems that operate critical energy infrastructure face increasingly severe and sophisticated cyber attacks from determined adversaries. To avoid disruptions to the nation's critical energy functions, energy systems must be engineered to withstand intentional cyber compromise, exploitation, and misuse.

While traditional engineering includes considerable safety and failure mode analysis, these risk management approaches rarely address the risks introduced by an intelligent and capable adversary with the goal of denying, disrupting, or destroying a critical function using cyber means. Most cybersecurity solutions are "bolted on" late in the engineering lifecycle, rather than intrinsically built into the system design.

The Opportunity of Cyber-Informed Engineering

Cyber-informed engineering (CIE) offers an opportunity to "engineer out" some cyber risk across the entire device or system lifecycle, starting from the earliest possible phase of design—the most optimal time to introduce both low cost and effective cybersecurity approaches.

CIE is an emerging method to integrate cybersecurity considerations into the conception, design, development, and operation of *any* physical system that has digital connectivity, monitoring, or control. CIE approaches use design decisions and engineering controls to mitigate or even eliminate avenues for cyber-enabled attack, or reduce the consequences when an attack occurs.

National CIE Strategy Directive

Enacted into law on December 20, 2019, Section 5726 of the *National Defense Authorization Act for Fiscal Year 2020* directed the Secretary of Energy to establish a government-industry working group to accomplish a series of tasks, including to develop a national cyber-informed engineering strategy to isolate and defend energy infrastructure from security vulnerabilities and exploits in the most critical systems. The Securing Energy Infrastructure Executive Task Force developed this National CIE Strategy for adoption by the Department of Energy.

While specialized information technology (IT) and operational technology (OT) cybersecurity experts bring strong cybersecurity capabilities to securing today's energy systems, many of the engineers and technicians who design and operate these energy systems currently lack sufficient cybersecurity education and training to engineer systems for cybersecurity from the outset, in the same way they engineer these systems for safety.

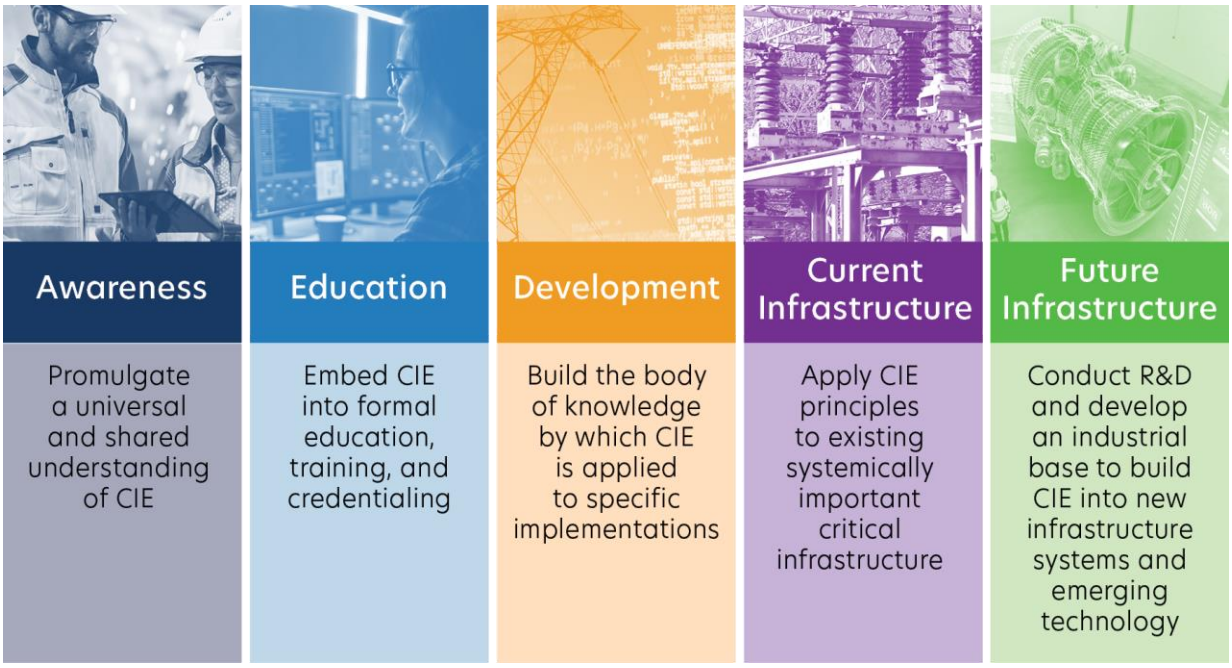
A National CIE Strategy for Energy

Pursuant to congressional direction,[2] the U.S. Department of Energy and the Securing Energy Infrastructure Executive Task Force have developed a strategy to enable the energy sector to lead the nation in incorporating CIE into the design and operation of infrastructure systems that rely on digital monitoring or controls.

[2] Section 5726 of the National Defense Authorization Act for Fiscal Year 2020.

The National CIE Strategy is built on five integrated pillars (see Figure 1), offering a set of recommendations to incorporate CIE as a common practice across the energy sector. Together, these approaches provide the body of knowledge, the diverse and expanded workforce, and the engineering and manufacturing capacity to apply CIE to today's energy infrastructure, and to engineer future energy systems to eliminate or reduce the ability of a cyber-enabled attack to succeed.

Figure 1. National Cyber-Informed Engineering Strategy



CIE provides the basis and approach for instituting a culture of cybersecurity within the energy industry, akin to the industry's strong culture of safety. Leading this cultural shift will be the engineers, industrial control system technicians, cybersecurity professionals, manufacturers, and owners and operators in the Energy Sector Industrial Base. The National CIE Strategy pillars provide a strong, integrated foundation to accelerate this cultural shift. The next step in moving CIE forward will be to convene a broad set of stakeholders to develop detailed implementation plans for each pillar of the strategy.

While this National Cyber-Informed Engineering Strategy has been developed for the energy sector, it can serve as a leverageable model for other critical infrastructure sectors to adopt and incorporate CIE into industry practices. CIE concepts and strategies include foundational engineering principles that apply to all types of engineering for critical infrastructure. Embedding CIE methods into the education and credentialing of the nation's next generation of engineers and industrial control system technicians will create a cyber-aware workforce that can design and manufacture resilient infrastructure systems across sectors.

CIE In Practice: Examples of Engineering Decisions Informed by Cyber Risks

CIE guides an engineering team to consider and mitigate the potential for cyber compromise throughout the engineering design lifecycle, leveraging engineering solutions to limit the pathways for cyber sabotage, exploitation, theft, and misuse within the system.

In a fully mature CIE design, requirements would be developed to describe not only expectations for how the system would function, but also specific high-consequence cyber impacts which must be prevented within the system design. During the design process, the team would make affirmative decisions about how to best accomplish those requirements, whether by enacting manual engineering controls, limiting digital functionality, employing operational cybersecurity solutions, or enacting monitoring schemes, or combinations of all the above. The risk of a future cyber compromise would be tracked and diminished as a fundamental engineering risk.

What does this mean in today's practice? The following hypothetical scenarios highlight the types of design changes and engineering decisions that could result from applying CIE during the design and build process:

- A 60-percent design review of a greenfield water treatment plant reveals that the design engineer replaced the manual hand-off-auto switches—which allow operations staff to run the plant manually—with a network-based communication device without manual overrides. The team elects to undo this modification, justifying the higher cost of construction with the benefit of assured manual controls in the event of a cyber compromise.
- A design team notes that the vibration trip sensor for a gas turbine is addressable on the same operational technology network with the turbine, and thus, could be compromised along with the turbine by an adversary who gains access to the network. Because this sensor is a safety feature for the turbine, the team chooses to deploy it on an isolated network—so that it is more inaccessible to cyber adversaries—and to employ a higher level of security controls, including a monitoring system, to heighten awareness of network anomalies affecting the sensor.
- A cyber exercise reveals the potential for a digital controller to be used to supply a harmful amount of treatment chemicals into a process, potentially causing damage to plant equipment. The engineering team is unable to remove the controller from service or to enact manual overrides, so they choose to adopt an engineering control limiting the chemical available to the process to an amount below the harmful level. This control is enacted through physical changes to the dispensing tank and documented in the Standard Operating Procedures.
- During the value engineering process for a wastewater treatment plant control system, the design team decided to save money by removing redundant hardwired controls and replacing them with digital input/outputs from the industrial controller. During a review, the engineering team noted that this decision would remove all manual operating capabilities from the pumps, meaning a successful ransomware attack on the control system could leave the pumps inoperable, resulting in potential spills and equipment damage. The project owner elected to absorb the additional cost in order to ensure the potential for manual controls in the event of a cyber attack.

Introduction

Currently, cybersecurity for most critical infrastructure control systems is addressed separately from system design and engineering. This gap has resulted in an ever-growing list of additive security technologies that are introduced after the fact to mitigate cyber vulnerabilities. Adding security technologies after the fact is more costly and less effective. What if critical energy infrastructure systems were designed and operated with cybersecurity built in, rather than bolted on after deployment? CIE provides a way to greatly reduce, and in some cases eliminate, cyber risks from the outset and increase overall efficiency and effectiveness.

CIE is an emerging approach that aims to integrate cybersecurity considerations into the conception, design, build, and operation of *any* physical system that has digital connectivity, monitoring, or control.[3] CIE can be broadly defined as: The inclusion of cybersecurity considerations as a foundational element of engineering risk management for any function aided by digital technology.

Today, engineers and industrial control system technicians build energy systems with specific goals for safety, reliability, and functionality. While systems engineering includes considerable safety and failure mode analysis, cybersecurity risks are often not specifically addressed—particularly the risks of intentional cyber compromise, exploitation, and misuse. Simply put, traditional engineering risk management approaches rarely address the risks introduced by an intelligent and capable adversary with the goal of high-consequence cyber-enabled impacts.[4]

CIE Linkage to Zero Trust and Secure by Design

Cyber-informed engineering embraces "secure by design" and "zero trust" software security strategies, and expands these concepts beyond software engineering to the engineering of cyber-physical systems.

Secure-by-design software development shifts the security focus from finding and patching vulnerabilities to eliminating design flaws in the architecture of a software system. CIE expands this concept to build secure architectures into physical infrastructure systems that have digital access or control.

A zero-trust architecture removes any implicit trust from devices or user accounts, moving away from the concept of a security perimeter that keeps attackers out. CIE embodies this approach by assuming that compromise is likely, and deploying resilient layered defenses that minimize the consequences possible when an asset or credential is compromised.

CIE represents the Department of Energy's strategy for implementing these approaches into energy infrastructure.

As a result, most cybersecurity solutions are introduced late in the engineering lifecycle, if at all, providing inadequate and more costly protection for the nation's energy industrial control systems (ICS). This approach misses significant opportunities to "engineer out" cyber risk—that is, using early design decisions and engineering controls to mitigate or even eliminate avenues for cyber-enabled attack, or reduce the consequences when an attack occurs. CIE embraces many complementary security approaches today, such as "zero trust" and "secure by design," conceptually extending them beyond application to software systems to include application to cyber-physical infrastructure.

CIE proposes a shift in focus in the way the nation's engineers, control system technicians, manufacturers, and operators approach security in energy systems design. Researchers began to define

[3] See more information on CIE at http://inl.gov/cie.
[4] High-consequence impacts, achieved using cyber means, that may disrupt energy sector functions that are critical to the nation.

the CIE approach in 2017.[5] in the intervening years, the federal government has supported several efforts that reduce cyber risks to the nation by applying CIE principles to critical energy infrastructure and new system designs. However, there is not yet a mature engineering discipline for identifying and addressing cybersecurity risk early in in the concept and design phases. There are also few commonly applied standards or guidelines to perform systems engineering risk management for ICS cybersecurity risks throughout the systems lifecycle.

CIE remains a promising approach that is not yet widely known, understood, or implemented. This National CIE Strategy offers an integrated set of recommendations to bring about the awareness, education, and resources to integrate CIE as a common practice within the Energy Sector Industrial Base.

Defining the Problem

Engineers—and the technicians who support the engineering process—are critical to the design, implementation, and secure operation of complex energy infrastructure and control systems. Even in this critical role, engineers often lack training, a body of knowledge, and other reinforcement of cybersecurity practices to effectively address cyber threats in energy infrastructure. Given the current and increasing criticality of digital control systems within critical energy infrastructure, this is a priority gap that must be addressed by the engineering community and the nation.

Current State

The adoption of digital technology into critical operational and engineering functions can introduce vulnerabilities that could compromise the availability, integrity, trustworthiness, or authenticity of the complex control systems serving those functions. Unless cybersecurity risks are explicitly considered within current approaches to hazard evaluation,[6] these vulnerabilities are not typically captured, missing critical opportunities to reduce or eliminate them during engineering and design. The engineers who oversee, invent, design, create, install, maintain, and dispose of these complex cyber-physical systems may lack the necessary requirements, context,[7] education, practices, and tools (in order of descending importance) to identify, understand, and mitigate these risks. Instead, engineers and the technicians who support them too often rely on the external application of cybersecurity measures by specialized practitioners late in the system implementation lifecycle. This current state

Alignment of CIE with Industry Standards and Guidelines

The National CIE Strategy will inform the evolution and maturation of industry standards and guidelines to align with CIE principles and provide manufacturers and asset owners with essential tools to demonstrate their adoption of CIE. Recent guidance shows strong alignment with CIE. Alignment with CIE can be an early target for the standards specification activities recommended in the Development pillar. Examples include the International Society of Automation (ISA)/International Electrotechnical Commission (IEC) 62443 series of standards, the National Institute of Standards and Technology (NIST) SP 800-160 guideline, and the SAE International G-32 Cyber-Physical Systems Security Committee standards work.

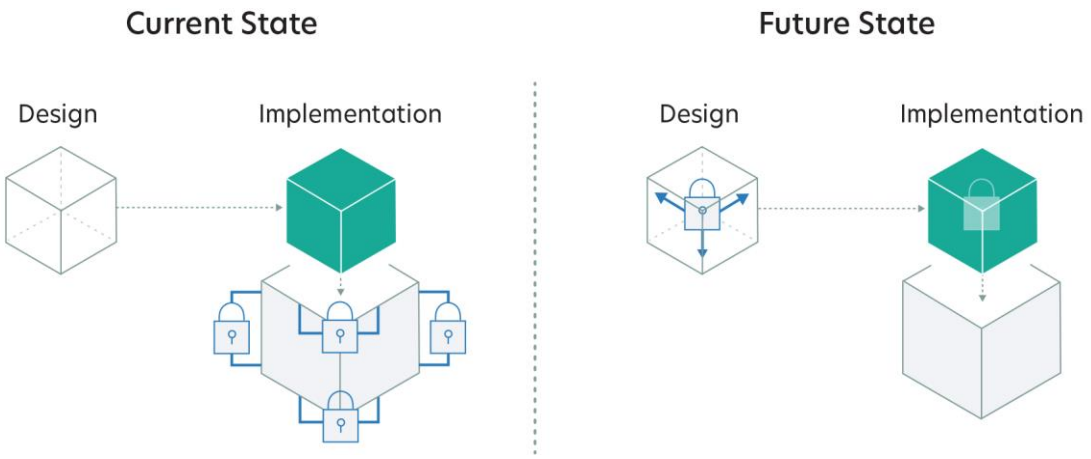
[5] Robert S. Anderson, Jacob Benjamin, Virginia L. Wright, Luis Quinones, and Jonathan Paz, *Cyber-Informed Engineering*, Idaho National Laboratory, 2017. doi:10.2172/1369373.
[6] Such as: failure modes effects analysis (FMEA), What-If analysis, hazard and operability study (HAZOP), fault tree analysis (FTA), and event tree analysis (ETA).
[7] *Context* refers to the broader environment in which the work of the engineer will be deployed for the benefit of society.

reduces the overall resilience and cost competitiveness of the systems supporting critical functions, increasing the risk of high-consequence cyber-enabled impacts that threaten national and economic security or public health and safety. This risk is magnified by the increase in well-resourced, sophisticated cyber adversaries who are targeting these cyber-physical systems to create damage or destruction.

Desired End State

What does CIE look like when fully implemented? Engineers incorporate cybersecurity practices into their body of knowledge, including engineering minimum requirements and specifications, for physical energy infrastructure systems that incorporate digital controls. Engineers and technicians fully evaluate the potential for disruption and harm from cyber attacks when designing and integrating digital components into energy systems. Control systems are chosen and integrated into physical systems only when a complete assessment of risks has been performed and the organization accepts any residual risk after being accurately informed of potential consequences. There is effective and continuing communication among owners, operators, designers, maintainers, device manufacturers, and system integrators to support risk-informed decisions concerning the use of control systems in energy infrastructure. Future technology is designed to be cyber resilient from the initiation of research through the development lifecycle. Cyber risk management early in the system lifecycle results in a more effective and efficient application of cybersecurity controls, and enables resilient operation of critical functions during potential cyber compromise. The broad range of stakeholders influencing energy infrastructure all are appropriately informed about cyber risks and have a culture of responsibility and agency for cybersecurity. Engineered systems are more cost-effective to operate securely over their life cycle, and security controls are more effective because they were built in at the design phase.

Figure 2. Current State vs. Desired End State

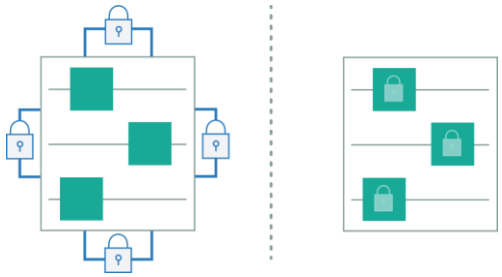


Principles of CIE

There are fundamental principles of CIE that should be considered for any energy sector infrastructure project that relies upon a digital industrial control system. By principles we mean the ideas, rules, or concepts that need to be kept in mind when solving an engineering problem. The principles identified here are not exhaustive but do serve as important elements within an ICS engineering risk management process. Principles identified as key considerations for CIE implementation are grouped into Design and Organizational principles, and are enumerated below.

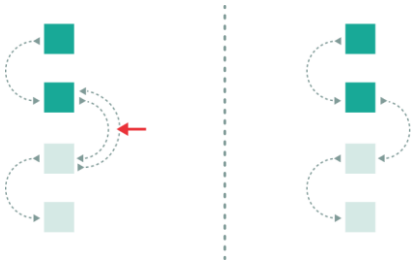
Design and Operational Principles

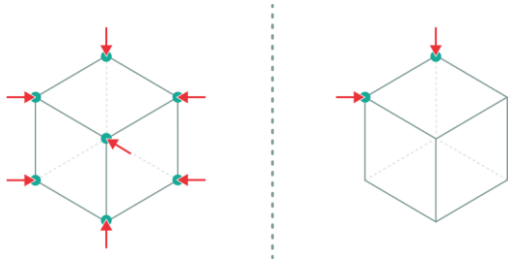
Consequence-Focused Design — Apply CIE strategies first and foremost to the critical functions where cyber manipulation could result in unacceptable consequences. Use a structured and thorough process to identify where cyber attacks may result in high-consequence impacts and examine how to avoid such consequences through secure design, implementation, and operation.



Engineered controls—Identify engineering changes and process controls early in system design to eliminate or mitigate cyber risk, reducing the need to bolt on additive IT security controls during implementation. Taken together, coordinated controls and processes are used to eliminate high-consequence cyber-enabled impacts. This requires integrating cyber experts and expertise into systems design, engineering, and modification.

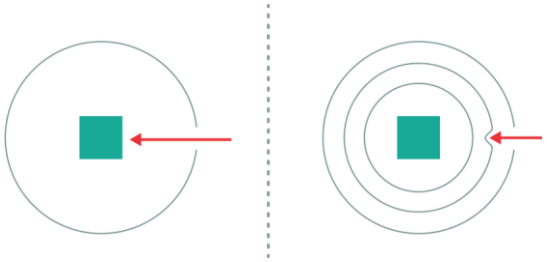
Secure information architecture—Design information pathways to ensure data flows only in desired ways and use proper architectural controls to enforce those information flows. This limits an attacker's ability to use the system or its information in undesired ways.



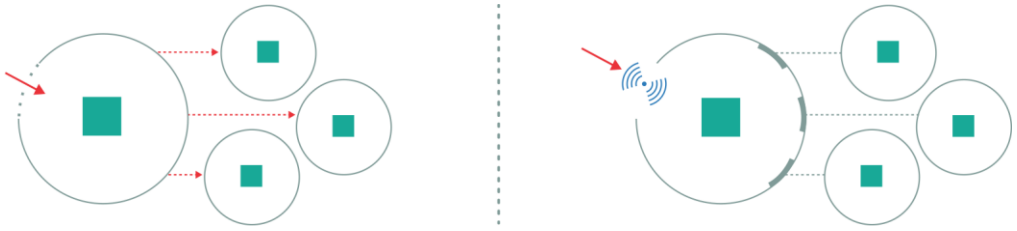


Design simplification—Simplify the system, component, or architecture design and limit high-consequence, low-value complexity within digital functions at the outset, reducing the opportunity for attackers to misuse digital functionality. Design simplification includes reducing latent capabilities in digital systems that operators may disable or may not even be aware of, but which attackers could leverage.

Resilient layered defenses—Assume compromise and employ a defense-in-depth strategy, reducing the opportunity for a single failure to impact critical functions or create cascading failures. This includes building in diversity, redundancy, and system hardening for adequate defense and predictable degradation during a cyber incident.



Active defense—Employ dynamic elements in the design of systems that detect and defend against cyber threats, enabling the system to continue operating resiliently when an intruder is detected, and isolate or remove the threat without compromising critical operations.



Organizational Principles

Interdependency evaluation—Integrate input from multiple disciplines and operational departments (e.g., safety, quality, maintenance, chemical) to understand how digital misuse could affect their area of operations. This ensures engineers can adequately plan for risks introduced by system interdependencies that may be outside of the engineer's traditional purview.

Digital asset awareness—Maintain a complete and accurate digital asset inventory, enabling engineers to track hardware, firmware, and software over time, and actively analyze the vulnerabilities that may reside within them.

Cyber-secure supply chain controls—Use procurement language and contract requirements to ensure that vendors, integrators, and third-party contractors deliver products that meet design specifications and adhere to organizational processes and controls that support cybersecurity.

Planned resilience with no assumed security—Expect that any digital component or system may be compromised at some point during its lifecycle, and plan for continued operation during and after a cyber attack that degrades digital controls. Implement a zero-trust architecture to the greatest degree possible.

Engineering information control—Protect sensitive engineering records—including requirements, specifications, designs, configurations, testing, etc.—that if released may provide attackers critical information that places those systems at greater risk.

Cybersecurity culture—Build cybersecurity into the organizational culture by leveraging a cross-functional and cross-disciplinary team to consider cyber-related concerns in the system design and implementation. Adopt continuous cybersecurity training across the organization to collectively empower all staff to participate in cybersecurity.

Key Premises of the National CIE Strategy

To safeguard U.S. energy infrastructure, the Securing Energy Infrastructure Executive Task Force recommends a National Cyber-Informed Engineering Strategy to fundamentally integrate cyber resilience into the design, implementation, operation, and maintenance of critical energy infrastructure and embedded energy systems in the United States. This National CIE Strategy is built on a few key assumptions:

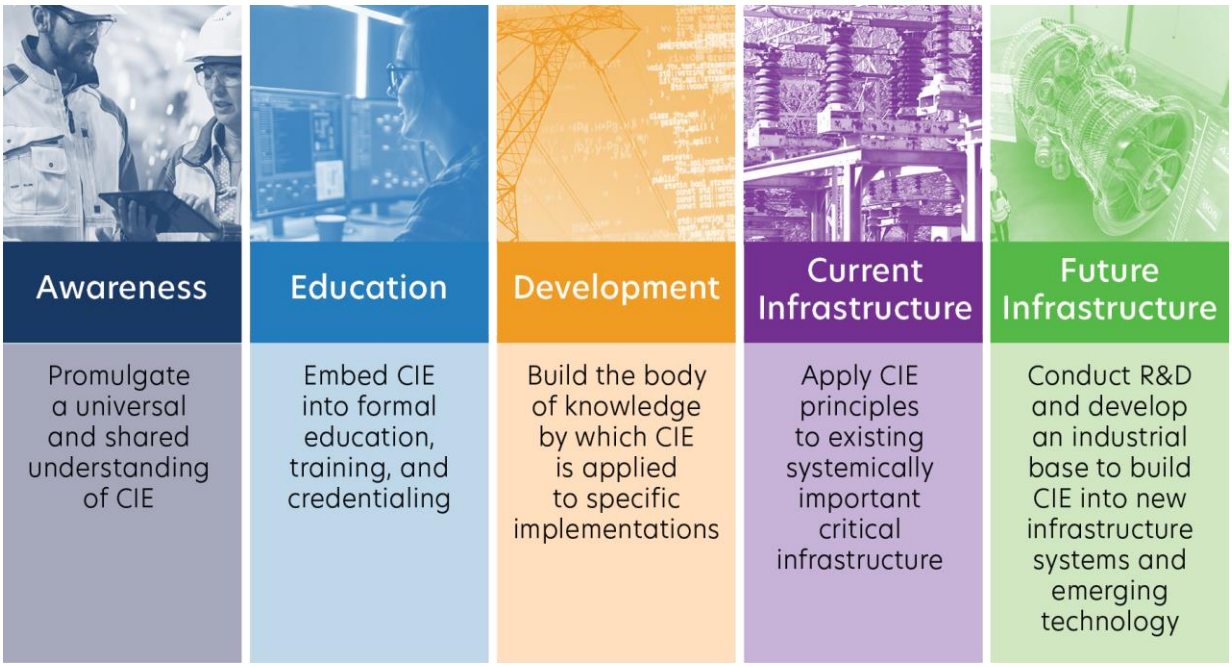
- Today's energy sector risk landscape calls for systems that are engineered to continue operating critical functions while faced with increasingly severe and sophisticated cyber attacks from intelligent, determined adversaries.
- While specialized IT and OT cybersecurity experts bring strong skills, many engineers and technicians who design and operate energy 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 the energy industry's adoption of a culture of cybersecurity by design—complementing the 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.

While this National Cyber-Informed Engineering Strategy has been developed for the energy sector, it serves as a template for other critical infrastructure sectors to adopt and incorporate CIE into industry practices. CIE concepts are not specific to any one sector, but rather represent foundational engineering principles that apply similarly to all critical infrastructure control systems.

Strategic Pillars and Recommended Actions

The National CIE Strategy is built on five integrated pillars. Together, these approaches enable the body of knowledge, the diverse and expanded workforce, and the engineering and manufacturing capacity to apply CIE to today's energy infrastructure, and to engineer future energy systems to eliminate or reduce the ability of a cyber-enabled attack to generate significant impact.

Figure 3. National Cyber-Informed Engineering Strategy



These five pillars represent parallel efforts that are closely intertwined; the recommendations for each often heavily support or directly feed into one another. Though this Strategy is focused on building CIE into energy infrastructure, it creates a blueprint for leveraging CIE to shift the culture of engineering in all U.S. critical infrastructure sectors.

The pillars of this National CIE Strategy define the pathways to achieving CIE. The next step in moving CIE forward will be to convene a broad set of stakeholders to develop detailed implementation plans for each pillar of the strategy.

Awareness

Promulgate a universal and shared understanding of CIE

Approach

Raise awareness of the CIE approach, its application potential, and major benefits among decision makers in the Energy Sector Industrial Base—including owners and operators, system engineers, manufacturers, researchers, and government leaders.

CIE requires a culture shift in the energy industry on par with the culture change for safety in engineering that has taken place over the last several decades. To initiate this shift, we must build an understanding throughout the entire energy infrastructure ecosystem of what CIE is, why it is needed, and how and where it can be applied.

CIE will require training and expertise, a shift in design and operational approaches, and engineering changes to the infrastructure that delivers energy functions critical to national and economic security. To build long-term support for and accelerate these changes, it is imperative that the nation's energy infrastructure decision makers understand CIE and its potential to limit the ability of cyber-based attacks to generate significant impacts.

Strategic Recommendations

1. **Lead a CIE awareness campaign to support a shift in the culture of energy infrastructure engineering and operations.**
   An awareness campaign should target the entire ecosystem of energy industry practitioners that must be engaged to build industry demand and embed CIE into engineering practices in the energy sector. This may include Congress, federal and state government partners, energy companies, trade associations, vendors and manufacturers, standards bodies, regulators, researchers, academic institutions, and more. An effective awareness campaign may include the following approaches:
   - Develop and implement an outreach strategy that builds national recognition and support for CIE. Leverage industry conferences, trade events, and published papers to build awareness of CIE concepts. Work with federal partners in the science and engineering community, such as the Department of Defense, and partners such as the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA), to develop and disseminate content on CIE principles and benefits.
   - Work directly with energy sector regulatory bodies, standards bodies, and trade associations to build recognition of the risk-reduction benefits of CIE. Consider where applying CIE practices can support manufacturers, owners, and operators.
   - Work directly with the Energy Sector Industrial Base to build recognition of the cost-benefit calculation and return on investment derived from implementing CIE.
   - Identify and cultivate champions of CIE within government, industry, and academia to socialize CIE concepts and generate community-wide discussion.
   - Engage the professional standards community to build support for and identify opportunities to include CIE in existing and new policies, standards, and guidance.

> "The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace.
>
> In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."
>
> **—Executive Order 14028, Improving the Nation's Cybersecurity, May 12, 2021**

2. **Formulate the technical requirements to implement CIE principles.**
   Engage stakeholders in the Energy Sector Industrial Base and beyond to develop and mature CIE principles and translate them into technical requirements that can inform CIE guidance, practices, and standards development. Socialize the technical requirements to differentiate CIE among established risk evaluation techniques and existing cybersecurity practices.
   - Engage standards bodies (e.g., National Institute of Standards and Technology (NIST), Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO), International Society of Automation (ISA), American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), American Society of Mechanical Engineers (ASME), SAE International), National Laboratories, manufacturing institutes, academic bodies, trade associations, and other stakeholders.

3. **Develop policy initiatives and build partnerships to incentivize the broad adoption of CIE in the energy industry.**

   Conduct an analysis of potential barriers and identify high-priority areas for policy development and partnership building with infrastructure owners/operators and manufacturers. Policy initiatives may include:

   - Grants and cost sharing to increase the adoption of CIE principles.
   - Education policy to encourage the development and integration of CIE curricula.
   - Support for guidelines and standards development.

4. **Develop and promote case studies that demonstrate the benefits of applying CIE to existing and emerging infrastructure systems.**

   Identify, document, and promote case studies and proofs-of-concept that demonstrate the application of CIE to critical functions performed in the energy sector in multiple types of applications.

   - Identify opportunities for pilot projects at Federally Funded Research and Development Centers, Manufacturing Institutes, and similar entities.
   - Demonstrate and document lessons learned, and use pilot experiences to support efforts to quantify benefits and identify the return on investment for owners and operators.

Education

Embed CIE into formal education, training, and credentialing

Approach

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

Building the workforce needed to apply CIE principles to the entire energy infrastructure ecosystem will require a multi-pronged approach. Navigating competing cybersecurity priorities in academia to build CIE into education and training will require a sustained effort, with strong support from not only trainers and educators, but also industry employers, who create the demand signal for skills. Building these resources can expand the diversity, capability, and capacity of the energy sector workforce.

Strategic Recommendations

1. **Create near-term CIE training and credentialing programs to rapidly produce a CIE-savvy workforce available to secure energy infrastructure.**
    - Develop a framework for CIE training that establishes learning outcomes and assessment tools, allowing for the flexible implementation of training programs at multiple institutions that support the same outcomes.
    - Incorporate CIE concepts into formal engineering credentialing programs, such as the Engineer in Training (EIT) and Professional Engineer (PE) certifications.
    - Support the development and publication of CIE online and in-person educational modules as open educational resources that can be freely adopted by colleges, universities, and training programs.
    - Leverage trade association networks to host CIE training programs and offer certifications for owners and operators and the vendor community.

2. **Partner with academia to embed CIE principles into appropriate courses and degree programs at the undergraduate and graduate levels.**
   Build CIE into formal education and certification for the next generation of energy systems engineers. This may include the following approaches:
    - Target a diverse mix of colleges and universities with a focus on multidisciplinary degree programs and work with educators to develop curricula that integrates CIE principles into engineering degree programs. Prioritize programs that will build greater gender, racial, and demographic diversity into the U.S. energy workforce.
    - Partner with accreditation and licensing bodies to nominate CIE principles for inclusion in criteria for engineering school accreditation (e.g., working with the Accreditation Board for Engineering and Technology [ABET]) and engineering certifications (e.g., the Engineer in Training [EIT] certification and Professional Engineer [PE] license).
    - Integrate standardized curricula for CIE into military academies, government training facilities, and private-sector cybersecurity training centers.
    - Work with the National Security Agency to develop a new designation for CIE as part of its National Centers of Academic Excellence in Cybersecurity program, which recognizes institutions that offer certain programs of study in cybersecurity.

3. **Partner with industry employers to ensure alignment between CIE curricula and certifications, and demand signals from employers.**
    - Identify key venues (e.g., trade associations, Manufacturing Institutes, etc.) in the Energy Sector Industrial Base as sources of input and validation of CIE curricula and certifications.
    - Establish a continuing engagement approach to elicit industry feedback and ensure alignment and evolution of CIE curricula and certifications.

4. **Identify and partner with Federal Programs that support engineering and technical workforce education to achieve inclusion of CIE principles and enrichment.**
   Some examples of federal programs include (but are not limited to):
   - The National Initiative for Cybersecurity Education (https://www.nist.gov/itl/applied-cybersecurity/nice)
   - The Minority Science and Engineering Improvement Program (https://www2.ed.gov/programs/iduesmsi/index.html)
   - The National Centers for Academic Excellence in Cybersecurity (https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/)

Development

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

Approach

Mature CIE approaches and promote broad application by building a repository of tools, practices, methods, and other enrichments that practitioners can draw upon to apply CIE to existing and new infrastructure and validate CIE applications. Document lessons learned from applying CIE principles to a diverse range of infrastructure at different levels of criticality and use those lessons to continuously develop and mature tailored guidance, case studies, and practices available to the Energy Sector Industrial Base.

Strategic Recommendations

1. **Leverage the DOE National Laboratories, academia, government partners, and industry to continually improve and expand the applicability of CIE.**
    - Apply CIE to a diverse mix of critical Energy Sector Industrial Base systems to build the body of knowledge and formalize CIE best practices. Identify and document success stories, case studies, and lessons learned that can continue building the overall body of knowledge. Demonstrate how best practices are tethered to foundational principles of engineering and cybersecurity.
    - Develop a method to quantify the benefits of CIE and the economic value of the consequences that are reduced or eliminated by applying CIE principles. Include guidance on how to adapt CIE approaches to various levels of system criticality, balancing the cost of implementation with the potential benefits.
    - Identify approaches to apply CIE principles to the design of high-quantity, low-value devices in the energy sector that may not individually justify significant CIE evaluations (e.g., distributed energy technologies). Address the complexities that arise when vulnerabilities in these devices have widely varying degrees of consequence depending on the system context for which the devices are deployed. Further consider situations in which telecommunication component designs may not be within the control of the CIE device owner.

CIE Strategy Alignment with National Policy

Recommendations in this National CIE Strategy identify actions that are aligned with and support critical policy thrusts for cybersecurity. For example, the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, released July 28, 2021, outlines the "need for security controls for select critical infrastructure that is dependent on control systems." It calls for the creation of cybersecurity performance goals for critical infrastructure to protect national and economic security along with public health and safety. As the National CIE Strategy moves into its implementation phase, alignment and support of high-priority cybersecurity and critical infrastructure resilience policies and guidance will be key to success.

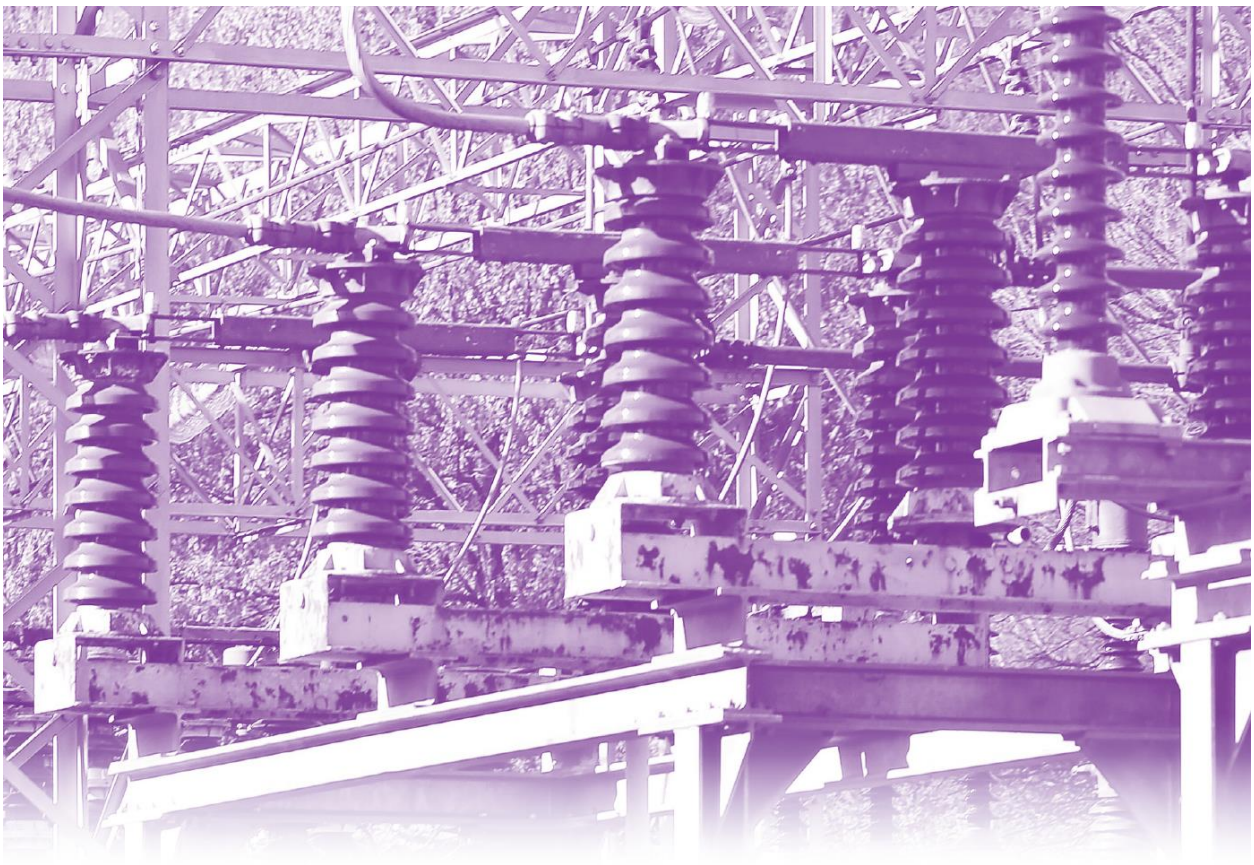
2. **Create and leverage a CIE Center of Excellence to execute the maturation of CIE.**
   A CIE Center of Excellence should be dedicated to conducting research to advance CIE approaches, developing guidance that supports training and implementation of CIE, extracting lessons learned from CIE applications, and transforming those lessons into new design approaches and philosophies for future installations. The Center of Excellence may pursue the following approaches:
    - Develop and continually refine guidance to support the implementation of CIE in existing and future energy infrastructure, including renewable energy systems.
    - Develop design specifications to align standards and guidelines to CIE principles and provide the specifications for manufacturers and asset owners to implement CIE. Support the evolution and maturation of existing standards and guidelines to align with CIE.

- Advance the development of reference architectures for ICS systems (to include examples developed by the Securing Energy Infrastructure Executive Task Force[8]) to demonstrate how CIE can be incorporated into the design of these systems.
- Leverage the new categories of security vulnerabilities for industrial control systems (developed by the Securing Energy Infrastructure Executive Task Force and being incorporated into MITRE's Common Weakness Enumeration framework[9]) to develop guidance that eliminates or reduces vulnerability categories for secure design and implementation in CIE.

3. **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.**
   Continuously contribute to and enrich a resource repository that will support CIE implementation, leveraging the outputs of the other pillars in this strategy. The repository will support engineers and operators of industrial control systems in both government and industry. Additionally, the repository will enable private sector leadership in CIE integration and will support a strong domestic Energy Sector Industrial Base developing cyber resilient systems and technologies.

   This library may include:
   - Guidance on implementing CIE in the design and engineering development process, including case studies that exemplify CIE approaches to diverse infrastructure applications.
   - An inventory of applicable standards and methods that support CIE and prioritize enhancements to enable and encourage CIE in other industry standards.
   - Lessons learned on vulnerable design patterns (identified in the Current Infrastructure and Future Infrastructure pillars).
   - Guidance on how to demonstrate and validate that CIE principles have been effectively applied to a project from R&D through implementation and operations.

[8] The reference architectures and new categories of security vulnerabilities are additional results of the work done by the Securing Energy Infrastructure Executive Task Force, which included members representing the federal government, energy asset owners and operators, energy system vendors and manufacturers, the academic community, and the National Laboratories. Section 5726 of the *National Defense Authorization Act for Fiscal Year 2020* directed the Secretary of Energy to establish the task force to carry out a number of tasks, including development of this National CIE Strategy. The reference architectures and new categories of security vulnerabilities for ICS will be included in the Task Force's forthcoming Final Report, expected in 2022.
[9] MITRE Corporation, "CWE," https://cwe.mitre.org/.



Current Infrastructure

Apply CIE principles to existing systemically important critical infrastructure

Approach

Use a consequence-driven approach to identify and apply CIE principles to the nation's systemically important critical infrastructure[10] already commissioned and in service today. This targeted approach can better secure existing infrastructure by both increasing costs to adversaries and denying their ability to inflict unacceptable consequences on the nation's critical functions.

[10] Systemically important critical infrastructure are the nation's most highly critical systems and assets within the critical infrastructure sectors, where compromise may have significant impacts on the economy, national security, and public health and safety.

Strategic Recommendations

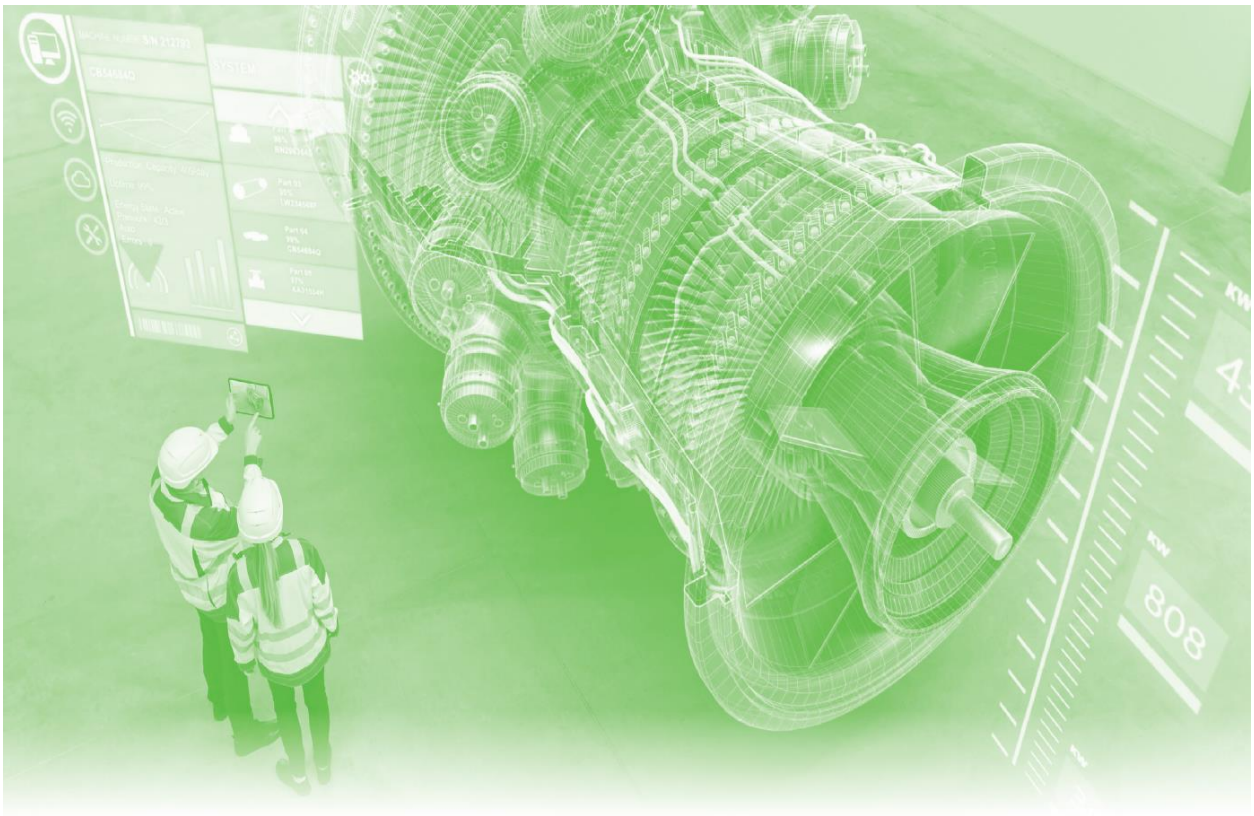
1. **Prioritize current infrastructure to apply CIE principles and identify needed upgrades.**
    - Develop a consequence-driven process to identify and prioritize existing infrastructure where applying CIE principles can best support national security. Identify installations where a cost-sharing approach is required to determine and implement necessary upgrades and mitigations to protect highly critical energy functions.
    - Investigate and develop CIE approaches and guidance that accelerate rapid and secure deployment of new clean energy technologies in the existing energy infrastructure.
    - Prioritize application of CIE principles to high-priority energy sector critical infrastructure, such as Defense Critical Electric Infrastructure.[11]

2. **Identify, document, and promote methods to apply CIE principles to reduce high-consequence impacts on a variety of existing infrastructure types that offer a high return on investment.**
    - Draw upon the guidance and reference architectures (called for in the Development pillar) to promote proven methods for owners, operators, and manufacturers to voluntarily apply CIE to existing infrastructure, where existing cybersecurity approaches do not meet CIE principles and guidelines.
    - Develop a "triage" process to identify the most appropriate applications for CIE and develop implementation plans and decision support tools that help owners, operators, and the vendor community asses when and how to apply CIE in current infrastructure and technology offerings.

3. **Develop methods to assess and validate the effectiveness of infrastructure upgrades and mitigations identified through CIE.**
    - Identify methodologies for asset owners and operators to validate and demonstrate that mitigations made, as appropriate, to infrastructure systems have reduced or eliminated avenues for attack.
    - Develop a framework that owners and operators can use to demonstrate where existing cybersecurity approaches meet CIE principles and guidelines.
    - Examine how to use assessments, such as Consequence-driven Cyber-informed Engineering (CCE), [12] for critical functions to both identify potential upgrades and validate that mitigations have been effective.
    - Develop tools, processes, and environments to facilitate validation in a minimally disruptive manner prior to deployment.

[11] Defined in Section 215A the Federal Power Act, as amended by the Fixing America's Surface Transportation (FAST) Act of 2015 (P.L. 114-94).
[12] DOE sponsored the Consequence-driven Cyber-informed Engineering (CCE) program at INL to develop a structured approach and tools to apply CIE-derived principles to infrastructure systems. See additional information at https://inl.gov/cce/.

4. **Embed CIE into procurement decisions and provide incentives to asset owners who invest in applying CIE principles to secure high-priority existing infrastructure.**
    - Develop grants and cost-sharing support to asset owners who conduct CIE reviews and invest in infrastructure upgrades.
    - Identify and pilot CIE-based procurement and integration strategies with one or more energy system operators. Publish lessons learned and a playbook to enable other system participants to embed CIE requirements into ICS procurement.



Future Infrastructure

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

Approach

Nurture and sustain an Energy Sector Industrial Base that enables manufacturers and asset owners to apply CIE principles into the full lifecycle (design, construction, operation, maintenance, and decommissioning) of newly commissioned critical infrastructure systems. The domestic industrial base will supply a sufficient diversity and quantity of resilient goods and services to include cybersecurity in existing engineering approaches and realize an infrastructure system built on CIE principles and strategies.

Achieving this vision requires a focus on conducting research and design of future energy systems using CIE, as well as supporting the technology and business ecosystem of how new systems are applied, operated, and maintained. Applying CIE principles and strategies offers the opportunity to grow a domestic manufacturing base of resilient energy systems and components, aligning to policy

recommendations directed in the Executive Order on America's Supply Chains (E.O. 14017), and DOE's report, "*America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition*," issued in 2022.[13] Applying CIE also leverages a strategic opportunity to establish and maintain leadership in advanced renewable energy systems that increase energy security and reduce emissions.

Strategic Recommendations

1. **Develop novel concepts for critical function assurance in emerging technologies—to include renewable technologies—that identify and revise design patterns that lead to high-consequence cyber-enabled impacts.**
   Existing cybersecurity standards and practices are implemented to support *information* assurance—protecting the confidentiality, integrity, and availability of information assets—rather than *critical function* assurance—eliminating opportunities to sabotage the delivery of a critical function.
   - Conduct R&D for novel system designs, renewable systems, and emerging technology built on CIE concepts.
   - Identify vulnerable design patterns in existing infrastructure (drawn from Current Infrastructure pillar activities) and develop and demonstrate new designs that eliminate these patterns.
   - Develop a CIE approach to design that considers the inherent risk of a global supply chain for commodity components, aligning to policies developed pursuant to E.O. 14017.
   - Conduct or leverage, as appropriate, existing R&D for design, control, and operation approaches based on CIE concepts to enhance critical function assurance for multistakeholder interdependent infrastructure system of the future.

2. **Drive the creation or revision of International Standards[14] for design, production, and lifecycle support capabilities to embody CIE principles.**
   - Develop reference implementations for ICS systems and components that incorporate standards supporting CIE principles.
   - Develop guidance for incorporating CIE principles at the design stage of next-generation embedded energy system devices.

3. **Provide market incentives that drive R&D and encourage domestic suppliers to apply CIE principles to their offerings as a long-term competitive advantage.**
   Provide the tools for system engineers to voluntarily demonstrate and assess their use of CIE principles in system design and implementation. This may include the following approaches:
   - Develop guidance for entities to perform an engineering and operations review to confirm CIE provenance, demonstrating that CIE principles were adequately considered throughout the project, from concept to R&D to implementation. Identify a "chain of custody" process to confirm due diligence in CIE throughout design and implementation.

[13] U.S. Department of Energy, *America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition*, February 24, 2022, https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition.
[14] Elements of an International Standard can be found at ISO, "Consumers and Standards: Partnership for a Better World," https://www.iso.org/sites/ConsumersStandards/1_standards.html.

- Develop metrics to assess the effectiveness of CIE application to lifecycle from conceptual design onward.
- Reduce deployment risk and lab-to-market cost by incorporating CIE principles in prototyping, integration testing, and validation of energy system devices with focus on new methodologies for computation and communications. These could include quantum computing, quantum-secure communications, 5G and 6G communications, and adversarial-robustness machine learning algorithm implementation for functional and supervisory controls.
- Provide insight into the business risk reduction and impact provided through application of CIE best practices.

4. **Prioritize federal support to national, state, and local infrastructure system projects designed, built, and maintained using CIE standards and approaches.**
    - Require the incorporation of CIE principles into federally funded R&D projects for energy infrastructure systems that ultimately include digital technology in their implementation or have an intersection with the ICS environment.
    - Prioritize federal funding to R&D projects that have a plan for incorporating and demonstrating CIE provenance throughout the project lifecycle.
    - Engage state public utility commissions, public service commissions, and other state regulatory bodies to integrate CIE requirements into their regulatory frameworks.
    - Enhance national energy security by developing CIE principles for application at regional and national scale—beyond the range of influence for any individual company or state regulatory body. Evaluate whether national CIE goals are achieved by infrastructure owners.

The CIE Strategy as a Model for Other Critical Infrastructure Sectors

Pursuant to congressional direction, the U.S. Department of Energy and the Securing Energy Infrastructure Executive Task Force[15] have developed this strategy to enable the energy sector to lead the nation in incorporating cyber-informed engineering into the design and operation of infrastructure systems that rely on digital monitoring or controls. Given the uniquely critical role of reliable energy to other all critical infrastructure systems, and to national and economic security, a national imperative exists to build resilience into critical energy systems at the earliest stages.

While this National Cyber-Informed Engineering Strategy has been developed by government and industry experts and researchers with specific experience in energy sector systems, the authors recognize that the recommendations herein have broad applicability to engineers and industrial control

[15] The National Cyber-Informed Engineering Strategy was developed by the Securing Energy Infrastructure Executive Task Force, which included members representing the federal government, energy asset owners and operators, energy system vendors and manufacturers, the academic community, and the National Laboratories. Section 5726 of the *National Defense Authorization Act for Fiscal Year 2020* directed the Secretary of Energy to establish the task force to carry out a number of tasks, including development of this National CIE Strategy.

systems across many critical infrastructure sectors. This strategy can serve as a guide for other critical infrastructure sectors to adopt and incorporate CIE into government and industry practices. CIE concepts and strategies apply to all types of engineering. CIE represents foundational engineering principles that apply similarly to all other critical sectors—such as water, transportation, telecommunications, manufacturing, and more. The energy sector heavily relies on these sectors to perform critical functions, creating an equal imperative to incorporate CIE into interdependent infrastructure systems. Indeed, results realized through the application of CIE principles and strategies will be optimized by adoption in other sectors, given the interdependencies among sectors.

Sector Risk Management Agencies, other Federal agencies, and critical infrastructure partners and stakeholders can leverage the National CIE Strategy as a model to implement CIE principles broadly to all U.S. infrastructure systems that operate critical functions for the nation.

Next Steps

Each of the five strategy pillars identifies a number of key actions, stakeholders, and alignments to address the gaps identified in the National CIE Strategy. These are broad actions that involve numerous organizations across government, industry, researchers, and academia. To organize this large set of stakeholders, develop and prioritize tactical actions, and implement CIE on a national scale an implementation plan is needed. Given the diversity of stakeholders required, forming a community of interest for each pillar of the strategy is recommended. These communities of interest can then develop detailed implementation plans for each pillar, identify champions within each pillar, identify resources and organizations to undertake critical activities, and outline the timeline and milestones for implementation.

Appendix A: Securing Energy Infrastructure Executive Task Force Participants

SEI ETF Direction

Cherylene Caddy, **Executive Director of the SEI ETF**, Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response,

Virginia Wright, **Technical Lead for the SEI ETF**, Idaho National Laboratory

Senior Executive Group

Sabrina Atack, Nuclear Regulatory Commission

Jim Beardsley, Nuclear Regulatory Commission

Manny Cancel, Electricity Information Sharing and Analysis Center (E-ISAC)

Frank Cilluffo, McCrary Institute for Cyber and Critical Infrastructure Security, Auburn University

Stan Connally, Southern Company

Joyce Corell, National Counterintelligence and Security Center, Office of the Director of National Intelligence

John Garstka, Department of Defense, Office of the Under Secretary of Defense for Acquisition & Sustainment

Alexander Gates, Department of Energy

Shana Helton, Nuclear Regulatory Commission

Patricia Hoffman, Department of Energy, Grid Deployment Office

Brian Holian, Nuclear Regulatory Commission

Bob Kolasky, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

Puesh Kumar, Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response

Mark Lauby, North American Electric Reliability Corporation (NERC)

Rick Ledgett, Center for Cybersecurity Studies, U.S. Naval Academy

Adrienne Lotto, New York Power Authority

David Revill, Georgia Systems Operations Corporation

Zachary Tudor, Idaho National Laboratory

Guy Walsh, National Security Collaboration Center, University of Texas at San Antonio

Dave Whitehead, Schweitzer Engineering Laboratories

Patrick Woodcock, Massachusetts Department of Energy Resources

Senior Technical Group

Christie A. Ansley Richard, Department of Defense

Dan Bennett, National Renewable Energy Laboratory

Freddy Blanco, Department of Defense

Sanjay Bose, formerly of the Department of Energy, Office of Electricity

Victor Costanza, New York Power Authority

Joseph Cummings, New York Power Authority

Iain Deason, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

Ben Deering, Office of the Director of National Intelligence

Jen Depoy, Sandia National Laboratories

Paul Forney, Schneider Electric

Brian Gaines, Sandia National Laboratories

Ismael Garcia, Nuclear Regulatory Commission

Vergle Gipson, Idaho National Laboratory

Nate Gleason, Lawrence Livermore National Laboratory

James E. Goosby, Southern Company

Howard Grimes, Cybersecurity Manufacturing Innovation Institute (CyManII)

Daryl Haegley, Department of Defense

Jordan M. Henry, Sandia National Laboratories

Andrew Kling, Schneider Electric

Steven Kunsman, Hitachi Energy

Arthur Lord, Department of Defense

Kathy Lyons-Burke, Nuclear Regulatory Commission

David Manz, Pacific Northwest National Laboratory

Tim Marshall, Dominion Energy

Carl McCants, Office of the Director of National Intelligence

Michael Mylrea, National Resilience, formerly of GE Research US

Jennifer Pedersen, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

Ryan Quint, North American Electric Reliability Corporation

Rick Raines, Oak Ridge National Laboratory

Edward Rhyne, formerly of the Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response

Mason Rice, Oak Ridge National Laboratory

Marc Sachs, Auburn University

Megan Samford, Schneider Electric

Nicholas Seeley, Schweitzer Engineering Laboratories

Paul Skare, Pacific Northwest National Laboratory

Kuan Wang, Department of Defense

Jonathan White, National Renewable Energy Laboratory

Technical Project Team: National CIE Strategy

Bob Anderson, Idaho National Laboratory

Matt Anglin, New York Independent System Operator (NYISO)

Craig Bakker, Pacific Northwest National Laboratory

Peter Bloniarz, New York Governor's Office

Samuel Chanoski, Idaho National Laboratory

Joseph Cummings, New York Power Authority

Michael Dransfield, Department of Defense

Will Edwards, Schweitzer Engineering Laboratories

Dennis Gammel, Schweitzer Engineering Laboratories

Ismael Garcia, Nuclear Regulatory Commission

Vergle Gipson, **TPT Chair**, Idaho National Laboratory

Jordan M. Henry, Sandia National Laboratories

Robert Hovsapian, National Renewable Energy Laboratory

Cynthia Hsu, formerly of the National Rural Electric Cooperative Association (NRECA)

William Hutton, National Rural Electric Cooperative Association (NRECA)

Dmitry Ishchenko, Hitachi Energy

Justin John, GE Research

Andrew Kling, Schneider Electric

Steven Kunsman, Hitachi Energy

Sin Ming Loo, Boise State University/Idaho National Laboratory

David Manz, Pacific Northwest National Laboratory

Carl McCants, Office of the Director of National Intelligence

Jeffrey Mitchell, Idaho National Laboratory

Mike Nygaard, Lawrence Livermore National Laboratory

Jennifer Pedersen, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency

Sean Peisert, Lawrence Berkeley National Laboratory

Stacy Prowell, Oak Ridge National Laboratory

Ryan Quint, North American Electric Reliability Corporation

Ron Ross, National Institute of Standards and Technology (NIST)

Michael Rowland, Sandia National Laboratories

Marc Sachs, Auburn University

Megan Samford, Schneider Electric

Steve Sanders, Southern Company

Greg Shannon, Cybersecurity Manufacturing Innovation Institute (CyManII)

Mike Smith, Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response

Curtis St. Michael, Idaho National Laboratory

Christopher Taylor, Southern Company

Stephen Trachian, Hitachi Energy

Kelli Urban, National Renewable Energy Laboratory

Alex Waitkus, Southern Company

Jonathan White, National Renewable Energy Laboratory

Virginia Wright, Idaho National Laboratory

Programmatic Facilitation and Support

KatherineAnne Baker, Nexight Group

Stephen Bolotin, Nexight Group

Lindsay Kishter, Nexight Group

Appendix B: Examples of CIE Implementation

Over the last few years, the U.S. Department of Energy, other Federal agencies, and industry, and academic partners have supported the development of structured approaches and methodologies to apply CIE principles to critical U.S. infrastructure. These approaches have been used to mitigate risks in existing infrastructure assets and "engineer out" risks in new system designs. A few examples are described below.

Consequence-driven Cyber-informed Engineering (CCE)

The Idaho National Laboratory has developed an approach to apply CIE to existing and new infrastructure builds with the support of multiple Federal agencies, including the U.S. Department of Energy and U.S. Department of Homeland Security. Consequence-driven Cyber-informed Engineering (CCE) is a methodology that implements CIE concepts through a thorough process of identifying and mitigating potential catastrophic effects of cyber-enabled destruction or disruption.

CCE begins with an assumption that a sophisticated and determined adversary *will* compromise an organization, but that it *is* possible to determine which functions could cause critical impact if manipulated, and to plan effective defensive measures against an adversary's interference.

To organizations deemed critical to U.S. national security, INL and DOE offer guidance, training, valuable expertise, and continuous support throughout a rigorous, year-long CCE engagement that involves four key phases.

- Phase 1: Consequence Prioritization—INL and the organization work together to determine potential high-consequence events that could cause critical adverse impacts.
- Phase 2: System-of-Systems Analysis—The CCE team then utilizes other CIE elements to identify details of the critical functions and the people, processes, and technologies used to implement them.
- Phase 3: Consequence-Based Targeting—This information is used in Phase 3 to identify unverified trust in the delivery of critical functions, as well as likely methods and means a sophisticated adversary could use against their unique infrastructure to achieve critical impact.
- Phase 4: Mitigations and Protections—Lastly, the CCE team will determine the most effective means of engineering out or reducing the risk of impact to those critical functions.

DOE has also supported the development of a self-driven version of the process known as ACCELERATE, which any organization can be trained to apply. A 16-hour preparatory training and workshop is available to support ACCELERATE initiatives.

CCE has offered a structured approach and guidance to apply CIE to existing infrastructure and engineer out some risk in electric, nuclear, natural gas, and military installations. The Development pillar in the National Strategy offers recommendations to continue building out the body of knowledge and demonstrated approaches to guide owners and operators in applying CIE to their critical systems.

For more information on the CCE methodology, visit https://inl.gov/cce/.

Integrating CIE into Nuclear Microreactor Design

CIE concepts have been exercised and implemented by design teams building new, groundbreaking nuclear microreactors for the U.S. Department of Defense. Idaho National Laboratory provided training to the design engineers on the CCE methodology, which leverages CIE principles to encourage the team to integrate cybersecurity into the final design. The design teams considered how an advanced adversary could potentially conduct cyber-enabled sabotage against the critical asset, and then how to incorporate engineering protections to avoid such sabotage. The use of CIE principles led to significant design changes, which can avoid additional cost, time, and risk versus implementing cybersecurity controls after operational functions are implemented.

Cybersecurity for the Operational Technology Environment (CyOTE™)

The Department of Energy is working with energy sector asset owners and operators (AOOs), partners, and INL to develop capabilities for AOOs to independently identify adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments. CyOTE™ seeks to tie anomalies in operations to the TTPs that indicate a cyber attack. By stringing together multiple techniques in the OT environment, AOOs can identify attack campaigns earlier, with more certainty, and with ever-decreasing impacts.

CyOTE™ offers a complementary approach to the CCE methodology. CCE and CyOTE™ are both designed to look for ways to mitigate risk in operating environments; CCE takes a path toward engineering solutions and protection, while CyOTE takes a path to improve detection in cases when an organization cannot effectively or affordably engineer out an identified cyber risk. CyOTE™ offers a methodology to mitigate that risk by building mature tools and processes to detect evidence of an attack and deploy resilient defenses.

For more information on the CyOTE methodology, visit https://www.energy.gov/ceser/cybersecurity-operational-technology-environment-cyote.

CIE in Education

As community awareness of CIE grows, universities are beginning to integrate CIE concepts into their engineering curriculum. For example, Boise State University will be offering a one-credit hour Cyber-Informed Engineering course beginning summer 2022. The Education pillar outlines a strategy for further building CIE into education, training, and credentialing programs.