

# *Cyber-Informed Engineering Research and Development Guide*

## ***Table of Contents***

<b>CYBER-INFORMED ENGINEERING (CIE) AND DEVELOPMENT GUIDANCE</b>	<b>3</b>
<i>Background</i>	4
<i>Motivation</i>	6
<i>Intended Audience &amp; Use of the Document</i>	7
Researchers	7
Program Managers	8
<i>Primer on CIE Principles</i>	9
<b>TARGETED GUIDANCE FOR RESEARCHERS</b>	<b>11</b>
<i>Stage Gate Approach for Innovation Management</i>	12
Stage 1: Idea Generation	12
Stage 2: Idea Screening	16
Stage 3: Business Analysis	20
Stage 4: Development and Testing	24
Stage 5: Prototype Development	28
<b>TARGETED GUIDANCE FOR FEDERAL PROGRAM MANAGERS</b>	<b>32</b>
<i>DOE Technology Readiness Levels and CIE Integration</i>	33
TRL 1-3: Basic Research to Proof of Concept	33
TRL 4-6: Technology Development to Prototype Demonstration	38
TRL 7-9: Prototype Deployment to Commercial Deployment	42
<i>Research and Development Guide Development Team</i>	46

## **DISCLAIMER**

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy LLC, for the U.S. Department of Energy under Contract No. DE-AC36-08G028308, and by Idaho National Laboratory, operated by Battelle Energy Alliance LLC, for the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517. Funding provided by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response.

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

The background features a light blue gradient with white circuit-like patterns on the left side. A large, semi-transparent padlock icon is centered behind the text.

***Cyber-Informed  
Engineering (CIE)  
Research and  
Development Guide***

# Background

This document provides guidance on incorporating cyber-informed engineering (CIE) principles into the research and development (R&D) of operational technology systems and tools, facilitating the creation and adoption of innovative technologies that are secure and resilient by design. As technological innovation and research in digital systems continue to have an increasing role in ensuring economic and national security, cybersecurity has emerged as a paramount concern across industries and sectors. The challenge of integrating robust cybersecurity measures is imperative to safeguard critical infrastructure, protect sensitive data, and preserve national security interests.

Traditional cybersecurity approaches for new and emerging technologies have primarily focused on reducing cyber risk by integrating cybersecurity solutions after the development of a technology is complete. However, this post hoc approach for addressing cyber risk not only misses key opportunities to enable these new technologies to be inherently secure and resilient, but it is also insufficient considering the increasing dependence of emerging technologies on digital systems and given an ever evolving and increasingly complex cyber threat landscape. CIE provides a proactive approach to addressing cybersecurity challenges throughout the R&D lifecycle of emerging technologies. CIE provides a set of principles and approaches that enhance the understanding of the cyber-induced high consequence impacts of the critical functions of a technology and how to integrate mitigation into its engineering, design decisions, and operational strategies. By adopting a CIE approach, researchers and innovators can systematically identify, assess, and mitigate the impacts of cybersecurity vulnerabilities at each stage of technology development, ultimately enhancing the security, resilience, and reliability of innovative solutions.

This document provides targeted guidance to researchers, innovators, and technology developers through key questions designed to help integrate CIE principles at each stage of R&D. It also includes key assessment metrics to evaluate the effectiveness and level of integration of CIE principles before progressing to the next stage. Additionally, this document offers similar guidance for federal program managers to help them integrate CIE principles into both the execution of research projects within their portfolios and the initiation of new research programs. This is achieved by developing funding opportunity announcements that leverage CIE principles. For researchers, the guide uses Robert Cooper's innovation management framework<sup>1</sup> to elucidate different stages of R&D. For federal program managers, the guide employs the US Department of Energy's (DOE's) technology readiness levels (TRLs)<sup>2</sup>.

Cooper's innovation management framework provides a structured approach to managing the R&D process for new and emerging technologies – from idea generation to technology adoption. By leveraging this framework, researchers can systematically integrate CIE principles into their R&D activities, ensuring that cybersecurity considerations are embedded into the innovation process from

---

<sup>1</sup> Cooper, R.G. (2015). The Stage-Gate® Product Innovation System: from Idea to Launch. In Wiley Encyclopedia of Management (eds C.L. Cooper, V.K. Narayanan and G. O'Connor). <https://doi.org/10.1002/9781118785317.weom130024>

<sup>2</sup> Technology Readiness Assessment Guide. <https://www.directives.doe.gov/directives-documents/400-series/0413.3-EGuide-04a-admchg1>

inception. Figure 1 presents the different stages of R&D in this framework, including the gates that each technology needs to pass through before moving to the next stage.

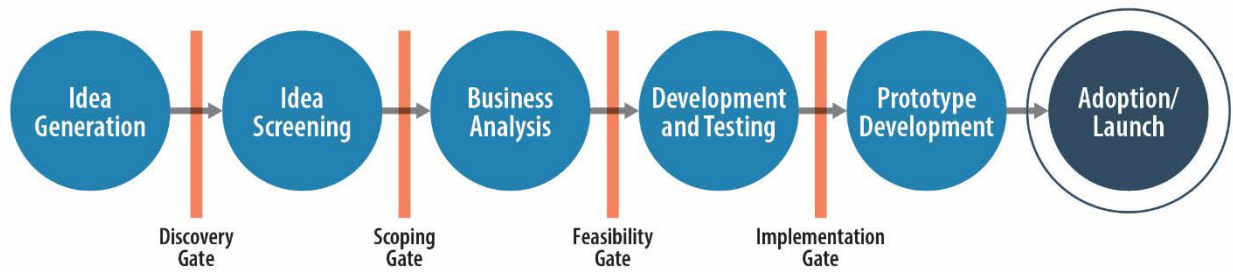


Figure 1: Innovation management framework

The DOE TRL framework offers a systematic method for assessing the maturity of technologies, ranging from basic research to commercial deployment. Program managers overseeing research programs can use the TRL framework to evaluate the readiness of technologies for real-world applications and to assess the integration of CIE principles into each stage of technology development. Figure 2 presents an overview of the DOE TRLs under different R&D efforts categorized based on their maturity level from a research laboratory to real-world adoption.

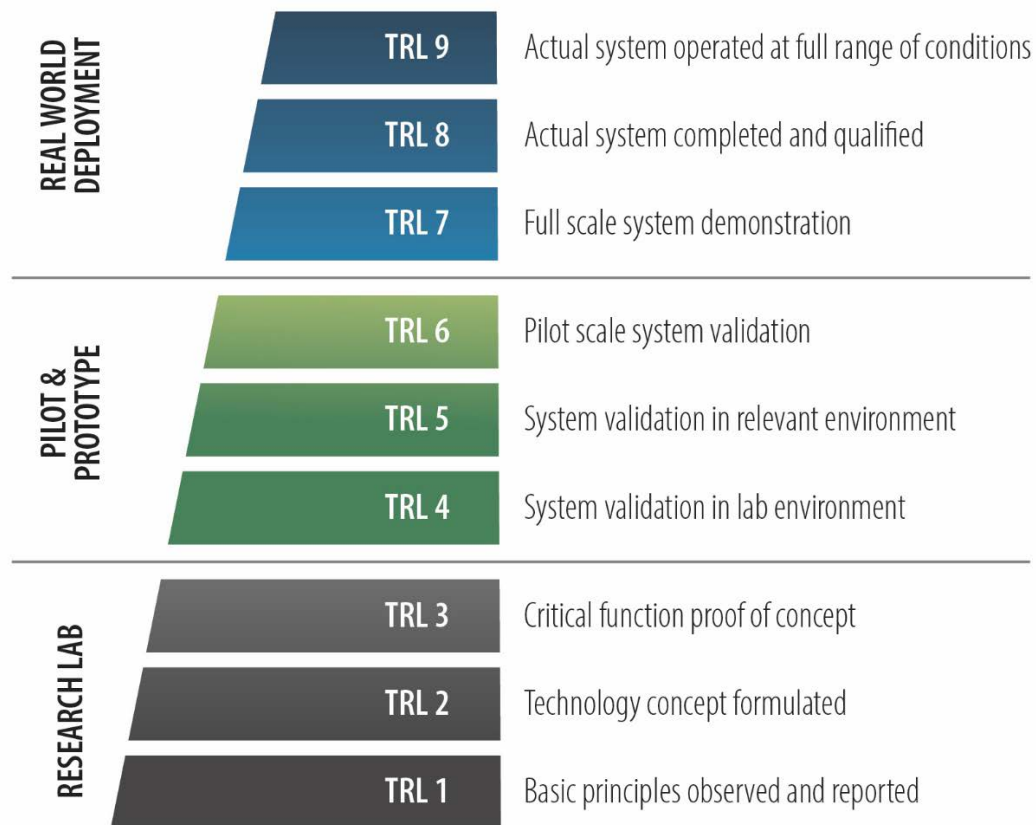


Figure 2: DOE Technology Readiness Levels

The motivation for using Cooper’s innovation management framework in conjunction with the DOE TRLs lies in their complementary nature: Cooper’s framework provides a structured approach for researchers to integrate cybersecurity considerations and CIE principles into their R&D processes, ensuring that cybersecurity is addressed holistically from ideation to implementation; and the DOE TRLs offer program managers a standardized method to integrate and evaluate the effectiveness of CIE principles across the stages of technology development at varying maturity levels.

## Motivation

The motivation behind this guide stems from a strategic imperative to address the escalating cybersecurity challenges facing our increasingly digitized world. As novel technologies and infrastructure continue to emerge at an unprecedented pace, so do the threats posed by malicious cyber actors seeking to exploit their vulnerabilities. The exploitation of new and emerging technologies not only results in slowing their adoption and reducing their impact, but also can have grave economic and national security consequences. In response to this evolving threat landscape and increasingly complex digital ecosystem, there is a need for a proactive and comprehensive approach to account for cybersecurity at the earliest stages of technology development.

The key recommendations in DOE’s National Cyber-Informed Engineering Strategy<sup>3</sup> (hereafter referred to as CIE Strategy) advocate for an approach that integrates cybersecurity considerations into engineering practices, design decisions, and operational strategies. The strategy recognizes that traditional approaches to cybersecurity, which often involve retrofitting security measures into existing operational technologies and critical infrastructure systems, are no longer sufficient. Instead, it calls for a paradigm shift toward “secure-by-design” technology development whereby possible impacts of adverse cyber events are accounted for at the earliest stages of technology conception while allowing for design and engineering mitigations to be deployed throughout the technology development process.

The imperative to make new operational technology secure-by-design is driven by several key factors:

**Protect critical infrastructure:** As critical infrastructure becomes increasingly reliant on highly interconnected and digital systems, the consequences of cyberattacks grow more severe. Ensuring that new technologies are secure-by-design is essential to safeguarding critical infrastructure—including electric grids, transportation networks, and healthcare systems—from cyber threats that could disrupt critical services and endanger public safety. Along with that the complex and ever evolving digital landscape makes it difficult to anticipate the new vulnerabilities that might be introduced in critical infrastructure systems. By baking security into the system right from the technology development stage can help minimize the impacts of uncertainties due to evolving vulnerabilities and cyber threats.

**Reduce barriers to new technology adoption:** With a focus on mitigating the impacts of inevitably successful cyberattacks by proactively designing and developing new operational technology systems—such as energy system technologies, aviation systems, and water systems—CIE principles

---

<sup>3</sup> National Strategy for Cyber Informed Engineering, U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, 2022. [https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022\\_0.pdf](https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf)

can accelerate the safe and secure adoption of new technologies. By incorporating security considerations into the engineering and design of the systems also allows for easier adoption by users who might not be well versed in the domain of cybersecurity.

**Promote innovation and economic competitiveness:** CIE principles not only enhance technology development that is inherently secure and resilient but also foster innovation and economic competitiveness. By instilling confidence in the security and reliability of new and emerging technologies, organizations can accelerate their adoption and commercialization, driving economic growth, and maintaining leadership in the global marketplace.

The motivation behind this guide is rooted in the recognition that cybersecurity cannot merely be an afterthought in the technology development process but rather a fundamental imperative from inception. This can be realized by acknowledging, especially in the early research stages, that there are strategic opportunities to identify and engineer cybersecurity and resilience into technologies. By embracing the CIE principles and striving to make new technologies secure-by-design, we can forge a path toward a safer, more resilient, digital future for all major industrial and economic sectors.

## Intended Audience & Use

This guide is a resource for two key audiences: researchers and federal program managers involved in R&D activities across a variety of critical infrastructure sectors and operational technology areas where there is heavy dependence on the digital infrastructure. Both audiences play a distinct yet critical role in advancing research innovations, and both have unique motivations and constraints. This document provides actionable guidance based on CIE principles to address the challenges of cybersecurity for new and emerging technologies from inception to adoption.

### Researchers

Researchers play a foundational role in technological innovation, driving discoveries and accelerating scientific advancements. This guide provides a comprehensive resource for researchers to integrate CIE principles into their R&D processes. Leveraging the stage-gate approach as the underlying structure, researchers gain a systematic method of incorporating cybersecurity considerations from ideation to implementation, to adoption, including considerations for the business analysis of new technologies considering CIE principles. This document also offers a noncomprehensive set of key questions and assessment metrics that align with each stage and gate of the framework, enabling researchers to proactively identify, assess, and mitigate cyber consequences as they progress through the different stages of technology development and R&D life cycle. Following are the key guidelines for effective use of this guide by researchers:

- Ideally, CIE principles should be considered at the initial stage of idea generation or inception of technology development, but researchers might encounter this guide while their efforts are at a different stage of the R&D life cycle. Researchers should leverage the key questions and assessment metrics from the stage that best aligns with their current R&D efforts. Regardless of the current state of R&D, researchers will still find this guide helpful in addressing cybersecurity considerations.



- The CIE principles-based key questions in this document are not intended to be comprehensive or compulsory. Researchers should leverage the key guidance questions for their R&D effort to explore the cybersecurity challenges and opportunities for mitigation at the relevant stage in R&D life cycle.
- Similarly, the assessment metrics at the end of every R&D life cycle stage are neither comprehensive nor compulsory. Researchers should leverage the assessment metrics to judge the level of integration of CIE principles at the given R&D stage. The selection of the proper assessment metric will need to be considered while accounting for the technology development area, and not all the assessment metrics listed in this document need to be addressed or quantified before the technology can move to the next stage of R&D.
- Finally, researchers should use this guide to advance the benefits of systematically integrating cybersecurity considerations into their R&D processes to enhance the security and resilience of their technological solutions. In practice, this involves assigning varying levels of importance to different key questions and metrics as the effort progresses through different stages of the R&D life cycle.

## Program Managers

Program managers play a pivotal role in initiating and overseeing research programs at varying levels of maturity that address the grand challenges faced by various sectors and enable the innovation and advancement of science. In addition, program managers ensure that their research programs align with organizational missions, goals, objectives, and budgets. This guide offers program managers a structured approach to integrate CIE principles into their research programs while leveraging the DOE TRL framework.

To account for the similarities in the maturity levels and the nature of activities for different TRLs, this document provides key questions and assessment metrics in three ranges of readiness levels: TRL 1–3, TRL 4–6, and TRL 7–9. Developing guidance based on the similar TRLs enables program managers to systematically and effectively integrate CIE principles for different research efforts into their portfolios—from fundamental research to more applied efforts of prototyping and technology demonstration. It also enables program managers to evaluate the efficacy with which the CIE principles are integrated into not only the final products or deliverables but also the proposal, execution, performance, and closeout phases of the research effort. By employing this guidance, program managers can enhance their ability to make informed decisions, effectively evaluate research proposals, strategically allocate resources, and ensure the successful development and deployment of novel technologies that are secure and resilient by design.

Following are the key guidelines for effective use of this guide by program managers:

- The CIE principles-based key questions and assessment metrics for different TRL ranges aim to be independent of each other, allowing for program managers to select the appropriate TRL range that best describes their research portfolio, and they are not meant to be interdependent.

- A single research portfolio or program might cross multiple TRL ranges presented in this document—e.g., from TRL 1 through TRL 6—so the program manager should leverage the guidance from the relevant TRL ranges. The guidance aims to help program managers integrate CIE principles and assess their efficacy while assisting their research programs as they progress through multiple TRLs.
- Neither the CIE-based key questions nor the assessment metrics are intended to be comprehensive for different TRL levels. This guide should be leveraged as a starting point and a tool to assist program managers to develop a comprehensive CIE integration and assessment plan for their research portfolios.
- Ideally, CIE principles should be integrated at the initiation stage of the research effort, such as by developing and including CIE-based requirements in funding opportunity announcements and proposals, but that might not always be feasible. Program managers should leverage this guide to identify the strategic stages of their programs where integrating CIE would be the most beneficial considering the budget, the nature, the maturity, and the end goal of the research.
- Finally, program managers should use this document to enable R&D efforts that result in innovative technologies that are secure and resilient by design. The document should be considered descriptive rather than strictly prescriptive, guiding the realization of these eventual benefits.

## Primer on Cyber-Informed Engineering Principles

This section provides a brief primer on the CIE principles that are leveraged to develop the targeted R&D guidance for researchers and program managers. For a more detailed understanding and application of these principles, refer to CIE Strategy and the Cyber-Informed Engineering Implementation Guide<sup>4</sup>.

1. ***Consequence-focused design***: Identify and mitigate cyber-induced, high-impact consequences during the design phase of technology development.
2. ***Engineered controls***: Identify, design, and implement engineering solutions that specifically aim to mitigate key high-impact, cyber-induced consequences.
3. ***Secure information architecture***: Ensure that key data flows for critical technology functions are identified and a secure information architecture is developed and implemented to secure the data flows.
4. ***Design simplification***: Identify the key design features that are necessary for the critical functions of the proposed technology. Simplify the design to reduce complexity; to reduce

---

<sup>4</sup> Virginia L. Wright et al., "Cyber-Informed Engineering Implementation Guide" (United States, 2023), <https://www.osti.gov/servlets/purl/1995796>

cyber-induced, high-consequence impacts; and to reduce the potential attack surface of the digital technology.

5. **Layered defenses:** Identify and deploy diverse and redundant defense measures to enable a robust defense-in-depth strategy for the technology.
6. **Active defenses:** Identify and deploy proactive and dynamic cyber defense measures in the design and deployment of the technology.
7. **Interdependency evaluation:** Identify and assess the key interdependencies of critical functions within the technology and the interdependencies with the broader system of systems for deployment.
8. **Digital asset awareness:** Identify and monitor the digital assets and assess the common cyber weakness of the key digital assets on which critical system functions of the technology depend for both performance and adoption.
9. **Cyber-secure supply chain:** Ensure that the procurement and supply chain practices for the key components of the technology are secure and resilient and that protections are in place to prevent the identified high-impact consequences.
10. **Planned resilience:** Without assuming the inherent security of any components, develop and design operational strategies for the continued operation of key technology features and functions while withstanding adversary attacks.
11. **Engineering information control:** Identify and protect the critical design and engineering information generated for the technology, from conception to adoption.
12. **Cybersecurity culture:** Foster an R&D culture throughout the R&D life cycle that promotes cybersecurity awareness for everyone involved.



***Targeted Guidance  
for Researchers***

# Stage Gate Approach for Innovation Management

## Stage 1: Idea Generation

At the idea generation stage, researchers explore multiple concepts and approaches to address a particular need or challenge. CIE principles can be leveraged by encouraging innovators to consider cybersecurity challenges during the initial stages of idea generation. By incorporating cyber consequence analysis and engineering-based mitigation strategies into brainstorming sessions, researchers can proactively identify potential cybersecurity challenges and opportunities for secure design solutions. The research efforts at this stage can be generally characterized by the following key activities:

- Brainstorm and explore multiple new ideas and concepts with a focus on addressing the key challenges or needs.
- Conduct extensive literature reviews and data collection to understand existing knowledge and identify gaps.
- Clearly articulate problems or opportunities, emphasizing the identification of critical functionalities and features.
- Develop initial hypotheses or research questions that consider cybersecurity challenges.
- Maintain a flexible and iterative approach to refining ideas, continuously incorporating feedback and new insights.

### *Key Questions for Each Cyber-Informed Engineering Principle*

#### **Consequence-Focused Design**

What critical functions are associated with each proposed idea, and what are the potential consequences of cyber manipulations of these functions?

What high-consequence impacts resulting from cyberattacks on the technology leveraged for the idea can be identified at this phase? What priority should each have due to its severity?

What strategies and design considerations can be identified now that would mitigate cyber-induced, high-consequence events for each proposed impact?

#### **Engineered Controls**

What engineering changes and process controls could be integrated into the design of each proposed idea to mitigate cyber impacts?

Which engineering interventions to eliminate or reduce cyberattacks could be leveraged across multiple ideas and concepts at the initial stages of idea generation to provide deeper protections?

Where are the opportunities to integrate cyber experts into the ideation process to ensure that high-impact cyber challenges are considered at the outset?

### **Secure Information Architecture**

What are the critical data elements and flows that, if compromised or sabotaged, could result in a high-consequence scenario for each proposed idea?

Are there opportunities to leverage nondigital technologies for the verification of key data within the process or system?

Are there opportunities to design secure information architectures that protect critical data associated with each idea from unauthorized access or manipulation?

### **Design Simplification**

What design features are complex but necessary as they relate to dependencies on digital assets for each proposed idea?

How can the complexity of the proposed ideas be reduced to limit or eliminate opportunities for cyber-induced, high-consequence events?

Which specific design features or functionalities can be simplified to minimize the potential for misuse by attackers?

### **Layered Defenses**

What are some of the assumed cyber protections that could be applied to fully developed technology at scale? Are there any backup protections that can be added to the system to protect it when the main defense fails?

What defense strategies can be integrated into the design of each idea to provide redundancy and resilience?

Where are opportunities to incorporate diversity and redundancy into the design of the proposed ideas to eliminate or mitigate cyber-induced consequences?

### **Active Defense**

If the technology was developed to its operational scale, what roles would be involved in developing a strategy for defense? What assumptions are the design team making about how the defense of this design would work? Where should defenses be documented and exercised?

How confident are you in the identified active defenses at the ideation stage for each proposed idea?

What specific measures or processes can be incorporated at this stage of the research effort for each proposed idea that can enable the future identification and development of accurate active defense strategies?

### **Interdependency Evaluation**

On what other systems or functions does this technology depend? Where might a malfunction or misoperation on those elements cause a high-consequence event for this system?

How might the proposed ideas impact or be impacted by other operational components, systems, or systems-of-systems with which the proposed technology will be integrated?

What interdisciplinary perspectives are necessary to understand the interdependencies and mitigate the associated cybersecurity consequences?

### **Digital Asset Awareness**

What digital assets will be necessary in each proposed idea, and what are their criticality levels with respect to their impact on the critical functions of the proposed technology?

Are there weaknesses or vulnerabilities within the digital assets that need to be addressed during the idea generation phase?

### **Cyber-Secure Supply Chain Controls**

Will there be third-party components, services, hardware, or software that, if compromised, can induce identified high-consequence events for each proposed idea?

What critical functions for each proposed idea depend on third-party components or services?

What are the secure supply chain and sourcing challenges for each proposed idea?

### **Planned Resilience**

What are the consequences of the failure of critical digital assets for each proposed idea?

What are the different failure modes for each proposed idea?

What strategies will be implemented to ensure continued operation during and after a cyber-induced failure?

### **Engineering Information Control**

How will sensitive engineering records related to the design and development of each proposed idea be protected from unauthorized access?

What controls will be implemented to safeguard the design and engineering information throughout the idea generation and brainstorming process?

What specific requirements or regulations that govern the protection of engineering information need to be addressed?

### **Cybersecurity Culture**

How can a culture of cybersecurity awareness be fostered among team members involved in idea generation?

What cross-functional and cross-disciplinary teams will be established to consider the cyber-induced consequences to the systems and the cybersecurity concerns during the ideation phase?

Are there continuous cybersecurity training initiatives that can empower all staff to contribute to cybersecurity efforts?

### Assessment Metrics for Stage 1: Discovery Gate

- Number of critical functions identified for each idea and their associated potential consequences if compromised
- Technical soundness of mitigation strategies incorporated into ideas to address identified high-consequence impacts
- Complexity score assigned to each idea based on the level of simplification required to minimize potential cyber vulnerabilities and impacts
- Percentage of ideas with streamlined design features to reduce attack surfaces and potential misuse by attackers
- Number of cross-disciplinary inputs integrated into the idea generation process to assess potential interdependencies and associated cybersecurity scenarios
- Identification of critical interdependencies between digital and physical systems for each idea, along with mitigation strategies
- Accuracy and comprehensiveness of identification of failure modes for each idea, along with the efficacy of conceptual strategies for the continued operation of critical functions.



## Stage 2: Idea Screening

During idea screening, researchers evaluate the feasibility and viability of different concepts to determine which ones warrant further development. Integrating CIE principles into this process is critical because it will allow injecting cybersecurity considerations and opportunities into this decision stage. Researchers should assess each concept's feasibility and ability to address cybersecurity challenges and mitigate high-consequence events, ensuring that subsequent development stages, alongside other criteria, also incorporate CIE principles with the greatest potential for impact. The research efforts at this stage can generally be characterized by the following key activities:

- Assess the technical feasibility of the idea and determine if the necessary technological and personnel expertise is available or can be developed within the required time frame.
- Estimate the initial costs and resources required to develop the idea, including funding, personnel, and materials.
- Identify potential risks associated with the idea—including technical, market, and operational risks—and perform a preliminary risk analysis to gauge their impact and likelihood.
- Ensure that the idea aligns with the organization's or funding opportunity call's strategic objectives and goals. Assess its potential to contribute to long-term success and competitiveness.

### *Key Questions for Each Cyber-Informed Engineering Principle*

#### **Consequence-Focused Design**

Which screened ideas have the greatest potential for high-consequence impacts if subjected to cyberattacks?

How can ideas be prioritized based on their potential high-consequence cybersecurity impacts?

How feasible are the specific design features or functionalities across all the screened ideas that can be leveraged to mitigate or eliminate cyber-induced, high-consequence events?

#### **Engineered Controls**

What engineering changes or process controls are necessary to mitigate cyber-induced, high-consequence events for each screened idea?

How difficult is it to implement early engineering interventions to address potential cyber vulnerabilities and impacts across all the screened ideas? Can the ideas be prioritized based on the feasibility of implementing engineering controls?

What opportunities are there to integrate cybersecurity experts into the screening process to evaluate and prioritize the screened ideas?

#### **Secure Information Architecture**

Which screened ideas promise the most opportunities to develop a secure information architecture at the outset?

How feasible are the various architectural controls that are necessary to ensure data integrity and availability for critical functions associated with each screened idea?

Are there opportunities to enhance secure information architectures for screened ideas based on feedback from other operational or research experts?

### **Design Simplification**

Which proposed ideas provide the most opportunities for design simplification to mitigate cyber-induced, high-consequence events?

How feasible are the strategies to streamline digital functions within screened ideas while maintaining operational effectiveness?

### **Resilient Layered Defenses**

Can the different screened ideas be ranked based on their need for detailed defense-in-depth strategies to eliminate or reduce cyber consequences?

How feasible is it to integrate these layers of defense into the design of each idea to provide redundancy and resilience against cyber threats?

What are the cost and timeline impact to implement these layered defenses for each screened idea?

### **Active Defense**

How feasible is it to incorporate active defenses into the design of the proposed ideas to detect and mitigate against cyber threats in real time?

How will active defense mechanisms enable the resilient operation of the proposed ideas in case of a cyberattack?

Are there specific measures or protocols that can isolate or remove cyber threats and impacts without compromising the critical operations for each screened idea?

### **Interdependency Evaluation**

Which screened ideas have the potential to create dependencies or impacts on other operational assets or systems?

How will the research team prioritize ideas based on their interdependency evaluations, related consequences, and benefits?

Are there interdisciplinary perspectives that should be considered when screening and prioritizing ideas? Which disciplines need to be consulted?

### **Digital Asset Awareness**

What digital assets are associated with each screened idea, and what potential cybersecurity implications attend those assets?

What vulnerabilities within digital assets may influence the decision to proceed with or discard certain ideas?

What are the cost and timeline implications of integrating the digital assets for each of the proposed ideas?

### **Cyber-Secure Supply Chain Controls**

How will the research team evaluate the cybersecurity implications of the third-party components or services associated with each screened idea?

What criteria will be used to assess the cybersecurity readiness of vendors and third-party contractors? Can the screened ideas be prioritized based on vendor and contractor readiness and feasibility?

What are the specific cybersecurity requirements that potential suppliers must meet to be considered for further development for each screened idea?

### **Planned Resilience**

How will the research teams assess the resilience of each screened idea to potential cyberattacks?

How feasible are the measures that will be taken to enhance the resilience of the selected ideas during the screening process?

What are the cost and timeline impact of incorporating the planned resilience strategies for each screened idea?

### **Engineering Information Control**

How difficult is it to manage and protect sensitive engineering records related to each screened idea—both during the research effort and during the eventual adoption of the technology?

What controls will be implemented to ensure the confidentiality and integrity of the engineering information during the screening process?

### **Cybersecurity Culture**

How will cybersecurity awareness and best practices be integrated into the screening process for each idea?

What training or resources will be provided to team members to enhance their understanding of cybersecurity?

Are there opportunities to leverage cross-functional teams or collaboration platforms to facilitate discussions and decision making related to cybersecurity vulnerabilities and impacts during the screening process?

### **Assessment Metrics for Stage 2: Scoping Gate**

- Effectiveness of proposed engineered controls in reducing cyber vulnerabilities for screened ideas, measured through the feasibility assessment

- Level of integrating cyber experts into the screening process to ensure adequate consideration of engineered controls
- Completeness of digital asset inventory maintained for scoped ideas, including hardware, firmware, and software components
- Number of vulnerabilities and failure modes identified within digital assets associated with scoped ideas along with mitigation actions taken
- Evaluation of procurement language along with cost, timeline impact, and contract requirements to ensure alignment with cyber-secure supply chain principles for scoped ideas
- Effectiveness of supply chain controls in mitigating cyber vulnerabilities and related impacts associated with sourced components and services for screened ideas
- Ideas with the greatest opportunities for design simplification and planned resilience strategies.

### Stage 3: Business Analysis

During the business analysis stage, researchers assess the commercial potential and market feasibility of their concepts. CIE principles can inform this analysis by helping researchers incorporate the possible impacts of cybersecurity, along with cost and technology features, thus driving future market adoption and competitiveness. Researchers should evaluate how well each screened concept aligns with cybersecurity trends and industry standards that are relevant to the sector and technology area. By conducting a comprehensive business analysis through the lens of CIE principles, researchers can make informed decisions about the future integration and adoption challenges raised by cyber threats. The research efforts at this stage can be generally characterized by the following key activities:

- Conduct an in-depth analysis of the target market, including customer needs, market size, growth potential, and competitive landscape.
- Develop detailed financial projections, including cost estimates, revenue forecasts, profit margins, and return-on-investment analyses.
- Perform a thorough technical feasibility study, evaluating the technical requirements, the potential challenges, and the availability of necessary resources and expertise.
- Develop a robust business model and strategic plan, outlining how the product will be developed, marketed, and sold, including pricing strategies, distribution channels, and partnership opportunities.

#### *Key Questions for Each Cyber-Informed Engineering Principle*

##### **Consequence-Focused Design**

How can consequence-focused design principles be applied during the business analysis stage to identify potential high-consequence impacts of cyberattacks on critical functions?

What strategies can be employed to prioritize business initiatives based on their potential cybersecurity implications and consequences?

Are there specific design considerations that can mitigate the consequences of cyberattacks on critical business processes identified during the analysis?

##### **Engineered Controls**

How will engineered controls be integrated into the business analysis process to identify and mitigate cyber impacts associated with critical business functions?

What engineering changes or process controls are necessary to enhance the cyber resilience of business strategies identified during the analysis?

Are there opportunities to engage cybersecurity experts to assess and prioritize engineered controls for critical business initiatives?

### **Secure Information Architecture**

How can secure information architecture principles be applied during the business analysis stage to ensure the confidentiality and integrity of critical data?

What architectural controls are necessary to enforce secure data flows and prevent unauthorized access or manipulation of sensitive information?

Are there opportunities to enhance secure information architectures for critical business processes based on feedback from operational departments or cybersecurity experts?

### **Design Simplification**

How can design simplification principles be applied during the business analysis stage to optimize operational efficiency and mitigate cyber-induced, high-consequence events?

What design features or functionalities can be simplified to align with business objectives while enhancing the cybersecurity posture?

What opportunities are there to prioritize simplicity in business analysis decisions to minimize potential cyber vulnerabilities?

### **Resilient Layered Defenses**

What layers of defense are necessary to protect business assets and operations from cyber threats identified during the analysis?

Are there opportunities to establish redundant or fallback mechanisms to enhance the resilience of business strategies against cyberattacks?

### **Active Defense**

What active defense measures can be incorporated into the business analysis stage to detect and respond to cyber threats in real time?

How will active defense mechanisms be evaluated and refined based on feedback from the business analysis process?

Are there specific protocols or response procedures that should be developed to address cyber threats identified during the business analysis stage?

### **Interdependency Evaluation**

How might the proposed concept impact or be impacted by other operational departments or systems from a business perspective?

What potential interdependencies with existing business processes or market trends need to be considered during the analysis?

What interdisciplinary perspectives can improve the understanding of the business implications of the concept?

### **Digital Asset Awareness**

What digital assets are needed as part of the proposed technology adoption to sustain critical business functions?

How can researchers assess the digital assets' contribution to the proposed concept's market potential and competitive advantage?

Are there vulnerabilities within the digital assets that may affect the proposed concept's field adoption and commercial viability?

### **Cyber-Secure Supply Chain Controls**

How might third-party hardware and software components impact the proposed concept's business case or market adoption?

What measures based on business processes can ensure that the components of the proposed technology development are sourced from vendors and suppliers that meet the security requirements?

Are there specific contractual or procurement considerations related to cybersecurity that should be addressed during the business analysis stage of the proposed technology?

### **Planned Resilience**

What business policies and protocols can be developed that enhance the resilience of the key business functions against cyberattacks on the proposed technology?

What are the cost and timeline impact on the development of the proposed technology with an eye toward incorporating resilience strategies (e.g., redundancy)?

What business strategies can be incorporated to ensure the proposed technology's continued market adoption and growth in the face of cyber threats?

### **Engineering Information Control**

How can business processes and protocols be developed to ensure the protection of sensitive engineering records related to the proposed technology?

What engineering information can, if compromised, adversely impact key business functions after the adoption of the proposed technology?

What engineering information related to the proposed technology needs to be protected to ensure market adoption and competitiveness?

### **Cybersecurity Culture**

How will cybersecurity awareness related to the proposed technology be integrated into the business analysis process to enable resilient and secure technology development and adoption?

What training or resources will be provided to the research team to enhance their understanding of cybersecurity challenges and considerations from a business standpoint?

What opportunities exist to engage business strategy, market adoption, and regulation stakeholders and decision makers in discussions about the cyber consequences of the proposed technology's market adoption and commercialization?

### **Assessment Metrics for Stage 3: Feasibility Gate**

- Cost-effectiveness and robustness of proposed information pathways designed to ensure secure data flows and prevent unauthorized access or manipulation
- Evaluation of architectural controls to enforce secure information flows for critical business processes identified during analysis, including impacts on timeline and development cost
- Identification of potential cyberattack scenarios and planned resilience strategies for critical business functions
- Number of go/no-go decision points established in the project timetable based on planned resilience strategies and assessments
- Degree to which the business processes and policies support the sourcing of components and assets for the proposed technology development from supply chains that meet the security requirements
- Degree of cross-functional and cross-disciplinary collaboration needed in considering cybersecurity concerns during the business analysis stage
- Effectiveness of continuous cybersecurity training programs across the research teams in fostering a cybersecurity-aware culture
- Viability of the market adoption and commercialization of the proposed technology after key engineered controls and active defenses are incorporated into the development of technology.



## Stage 4: Development and Testing

In this stage, analyses from stages 1 through 3 are incorporated into a subset of concepts for further development and testing based on both the technical feasibility and the commercial viability of the technology. Integrating CIE principles at this stage is crucial for developing innovative technologies that are secure and resilient by design. Incorporating CIE principles can help researchers identify and test cyber-induced, high-impact scenarios and verify design and engineering-based mitigation strategies. The research efforts at this stage can be generally characterized by the following key activities:

- Develop an initial version of the technology to demonstrate and validate the core functionalities and design features.
- Conduct thorough technical testing and validation to ensure that the developed technology meets the specified requirements—functional, safety, and security—and resolve any issues or bugs.
- Engage potential users and stakeholders during testing to gather feedback on the usability, functionality, and security of the proposed technology, and use this feedback to make the necessary improvements.
- Iteratively develop and design the proposed technology to refine and enhance the technology based on the testing results and user feedback.
- Develop processes and testing plans to ensure that the developed technology complies with the relevant industry standards, regulations, and certifications, and address any gaps that are identified.

### *Key Questions for Each Cyber-Informed Principle*

#### **Consequence-Focused Design**

How can the accuracy of the cyber-induced, high-impact consequences be continuously identified and tested during the technology development?

How are the key features and critical functionalities being implemented, and what dependencies on the cyber systems are being introduced during the development of the proposed technology?

Are there specific testing scenarios or simulations that can be leveraged to evaluate the effectiveness and feasibility of the consequence-focused design measures during the initial development of the proposed technology?

#### **Engineered Controls**

What engineering and design decisions and controls can be developed at this stage to mitigate any cyber-induced, high-impact scenarios for the critical functionalities and features of the proposed technology?

What experimental studies or simulation studies can validate the effectiveness and comprehensiveness of the engineered controls to reduce key cyber-induced, high-impact consequences during the technology development?

What metrics need to be used to test and validate the effectiveness of the engineered controls of the proposed technology?

How do the engineered controls impact the key functionalities and features of the technology, and how can they be refined?

### **Secure Information Architecture**

What key information and data dependencies are being introduced during the design and development of the critical functionalities of the technology?

How can engineering and process enhancements ensure the integrity, availability, and timing of the data to support the critical functions of the proposed technology?

What testing and validation is needed to ensure secure data flows and prevent unauthorized access or manipulation of the information flows that are critical to the performance of the proposed technology?

### **Design Simplification**

What key design decisions drive the critical functionalities of the proposed technology?

What opportunities exist during the implementation of these design decisions to simplify the design and mitigate cyber-induced, high-impact consequences while maintaining critical functionalities?

How can the efficacy of the design simplification be tested and validated to reduce cyber-induced, high-consequence events and increase the resilience of the proposed technology?

### **Resilient Layered Defenses**

Based on the design and development of the key features of the proposed technology, what possibilities exist for cascading cyber-induced impacts?

How can principles such as diversity, redundancy, and system hardening be leveraged during technology development to minimize cyber-induced cascading failures across the critical functionalities of the proposed technology?

What testing and validation need to be performed to validate the effectiveness of the different layered defenses to reduce cyber-induced impacts and increase resilience without compromising the performance of the critical functionalities?

### **Active Defense**

What dynamic defense elements can be incorporated into the development of the proposed technology to detect and mitigate cyber threats and related high-impact consequences?

How can active defense measures be integrated into the design and development of the proposed technology to ensure that the critical functionalities of the proposed technology are resilient and secure?

Are there specific scenarios or attack vectors that should be simulated during testing to assess the performance of the active defense measures during the development and testing of the proposed technology?

### **Interdependency Evaluation**

What interdependencies of the critical functions with other systems and assets are being assumed and/or introduced during the design and development of the proposed technology?

Are there specific tests or simulations that should be conducted to evaluate and validate the need for, and accuracy of the development methods employed for the proposed technology in an interconnected system?

How will feedback from other departments be incorporated into the development and testing of the proposed technology?

### **Digital Asset Awareness**

What digital assets are being leveraged during the development of the critical functionalities of the proposed technology, and how will they be managed and monitored during testing?

What are the critical vulnerabilities of the digital assets used in the development of the proposed technology that can be identified during testing?

How will the research team track changes to digital assets and ensure their security and resilience features throughout the development and testing phase?

### **Cyber-Secure Supply Chain Controls**

How will the cybersecurity posture of third-party components or services used in the concept be validated during testing?

What are the dependencies based on the design and development of the critical functionalities of the third-party digital components?

What contingency plans are in place to address the security and resilience challenges in the supply chain of the critical components identified during the development and testing?

### **Planned Resilience**

What are the different cyber-induced failure modes that are the result of the development approaches of the critical functionalities of the proposed technology?

What are the possible fail-safe and fail-secure modes of the critical functionalities of the proposed technologies?

What measures can be introduced in the design and development of the proposed technology to ensure that the critical functionalities continue to operate securely and effectively under adverse cyber conditions?

### **Engineering Information Control**

What critical engineering information is being generated during the design and development of the proposed technology?

What controls are being put into place during the development and testing of the proposed technology to safeguard the critical engineering and design information?

What types of continuous testing and validation are needed to safeguard the critical engineering information of the proposed technology throughout the development and testing phase?

### **Cybersecurity Culture**

What protocols and training are in place to enable the continuous awareness of the cybersecurity challenges of the proposed technologies during the development and testing process?

Are there opportunities to conduct collaborative exercises or tabletop simulations to reinforce CIE principles and decision making during the development and testing?

### **Assessment Metrics for Stage 4: Implementation Gate**

- Validity and comprehensiveness of the high-consequence scenarios identified during the development and testing of the proposed technology
- Integration of defense-in-depth strategies into the testing and development processes to mitigate the impacts of potential cyberattacks
- Effectiveness of layered defense mechanisms in providing redundancy and resilience against cyber threats during testing
- Number of defense layers tested and validated for each development milestone, along with their impact on cyber resilience
- Number of successful cyber-induced consequence mitigations or removals achieved without compromising critical operations during testing
- Implementation of controls to protect sensitive engineering records, including requirements, specifications, designs, and configurations
- Effectiveness of information control measures and architectures to ensure that critical technology functionalities are not impacted due to adverse cyber events
- Compliance with protocols and procedures to manage and safeguard engineering records during testing and development.

## Stage 5: Prototype Development

Building on the advancements made in the development phase and lessons learned from testing the proposed technology, in the prototype development phase, researchers focus on refining the design and development of the proposed technology and on resolving challenges in the integration, adoption, and usability of the proposed technology. Researchers should leverage CIE principles to identify and anticipate cyber-induced, high-consequence scenarios during the integration and field deployment of the technology and to develop engineering strategies and design modifications to mitigate these scenarios. By integrating CIE principles into the prototype development, teams can build a strong foundation for secure and resilient technologies. The research efforts at this stage can be generally characterized by the following key activities:

- Finalize the detailed design specifications and technical requirements based on feedback from earlier development and testing stages.
- Develop a fully functional prototype that closely resembles the final product in terms of functionality, performance, usability, and security.
- Conduct comprehensive integration and deployment-based testing and validation of the prototype, including tests of performance and reliability, to ensure it meets all requirements and standards.
- Perform user acceptance testing with a broad group of end users to validate the prototype's effectiveness, usability, and satisfaction levels, and incorporate user feedback into the product refinement.
- Identify challenges to commercial manufacturing and production by developing detailed manufacturing plans, evaluating secure supply chain solutions, and establishing quality control processes.

### *Key Questions for Each Cyber-Informed Engineering Principle*

#### **Consequence-Focused Design**

What are the potential cyber-induced, high-consequence impacts to the critical functionalities of the technology prototype?

What design modifications or resilience strategies can be incorporated into the development and refinement of the prototype to reduce the consequences of cyberattacks?

What are the specific integration and deployment testing scenarios or simulations that can be used to evaluate the accuracy and comprehensiveness of the cyber-induced, high-consequence scenarios for prototype concepts?

#### **Engineered Controls**

What engineered controls can be implemented in the prototype development stage to mitigate cyber impacts and enhance resilience?

What tests or experiments can validate the effectiveness of the engineered controls to reduce the cyber impacts on the technology prototype?

Are there opportunities to refine the engineered controls based on feedback from the testing and validation of the technology prototype?

### **Secure Information Architecture**

What are the critical information pathways to enable the effective functioning and integration of the prototype in the field? What critical functionalities of the prototype depend on these pathways?

What measures can be implemented in the development and integration of the prototype to enforce secure data flows and prevent unauthorized access or manipulation?

What specific integration and deployment tests can assess the robustness of secure information architectures for the developed prototype?

### **Design Simplification**

How can the design be simplified at the prototype development phase to reduce or eliminate adverse cyber impacts on critical functionalities?

What design simplification decisions during the prototype integration can either mitigate or eliminate cyber-induced consequences?

What are the impacts of design simplification choices to enhance the security and resilience of the critical functionalities of the prototype?

### **Resilient Layered Defenses**

What are the cyber-induced failure modes for the developed technology prototype? How can these failure modes be validated?

What layers of defense are necessary to safeguard prototype concepts from potential cyber impacts?

Are there opportunities to strengthen layers of defense based on feedback from the testing and validation during the field integration and deployment of the prototype?

### **Active Defense**

What dynamic elements can be incorporated into a prototype to enable defense against cyber threats and anomalies?

How will active defense mechanisms be tested and validated during the prototype development to ensure their effectiveness in detecting cyber threats and mitigating consequences?

Are there specific scenarios or attack vectors that should be simulated during the integration and deployment testing to assess the performance of the active defense measures for the developed prototype?

### **Interdependency Evaluation**

What dependencies with other systems and assets need to be accounted for to ensure effective development, integration, and deployment of the technology prototype?

What potential interdependencies with existing processes or infrastructure need to be considered?

What interdisciplinary perspectives are necessary to ensure the prototype's effective and secure integration, deployment, and use?

### **Digital Asset Awareness**

What digital assets are involved in the prototype development as it relates to the critical functions for the prototype and what are their impacts on cyber induced high consequence scenarios?

How will the prototype development team ensure the integrity and security of digital assets throughout the prototype development and integration process to mitigate high consequence scenarios?

### **Cyber-Secure Supply Chain Controls**

How will the cybersecurity posture of any third-party components or services used in the prototype be evaluated?

What measures will be taken to ensure that vendors and third-party contractors adhere to cybersecurity requirements during the development, integration, and deployment of the prototype?

Are there specific tests or evaluations that can enhance the security and resilience of the supply chain for components used in the prototype development?

### **Planned Resilience**

What are the different fail-safe and fail-secure modes of the prototype?

What specific engineering and design decisions can be made during prototype development stage to enable resilience and redundancies?

What integration and deployment strategies can ensure the continued operation of the critical functionalities of the prototype in case of a cyber incident?

### **Engineering Information Control**

How will sensitive engineering records related to the prototype be managed and protected during the development and testing?

What controls can enhance information sharing and safeguard critical engineering information from unauthorized access or disclosure?

### **Cybersecurity Culture**

How will cybersecurity awareness be promoted among team members involved in the prototype development?

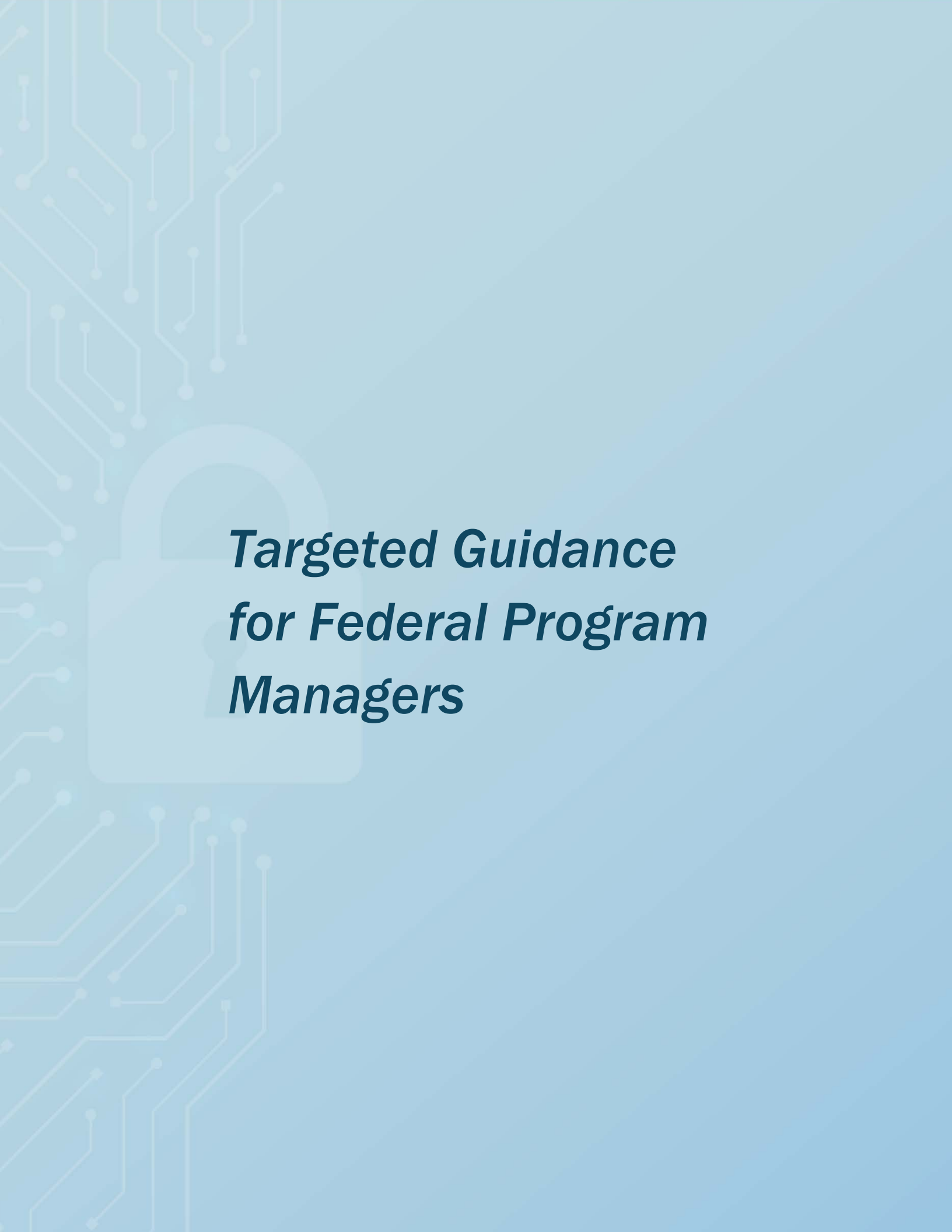
What critical information needs to be conveyed from the development and testing teams to the prototype development team to ensure appropriate cybersecurity awareness throughout the prototype development phase?

Are there opportunities to conduct collaborative exercises or simulations to reinforce cybersecurity concepts and decision making during the prototype development phase?

#### **Assessment Metrics for Gate 5: Integration and Validation**

- Evaluation of prototype designs to minimize the potential impacts of cyberattacks on critical functions identified during development
- Effectiveness of design modifications or resilience strategies in reducing the consequences of cyberattacks on prototype implementations, integration, and deployment
- Validation of engineered controls through tests or experiments to assess their effectiveness in reducing cyber impacts on the prototypes
- Effectiveness of design refinements based on feedback from testing and validation activities to improve engineered controls
- Enhancements to secure information architectures for prototypes to ensure data integrity and minimize adverse cyber impacts to critical functionalities of the prototype
- Validation of information pathways to enforce secure data flows and prevent unauthorized access or manipulation during prototype development
- Assessment of cyber-secure supply chains for the critical components used in the development and testing of the prototype.





***Targeted Guidance  
for Federal Program  
Managers***

# DOE Technology Readiness Levels and CIE Integration

## TRL 1-3: Basic Research to Proof of Concept

At TRLs 1–3, researchers conduct basic or theoretical research and generate proofs of concept to either answer the challenges in the domain or advance the state of the fundamental science and technology for the sector. These research efforts span from the exploratory research and observation of basic principles to the formulation of hypotheses and key research questions and R&D at both the analytical- and lab-level experimental efforts. Federal program managers in this TRL range play a crucial role in identifying key challenges and priorities facing the sector or field, driving innovation and encouraging multidisciplinary collaboration.

These stages provide the most opportunity for program managers to leverage CIE principles to develop innovative solutions and technologies that are secure and resilient. By leveraging CIE principles, program managers can also assess cybersecurity considerations in their research proposals, research plans, and project executions. Embedding CIE principles in research activities at these early stages can proactively address cybersecurity challenges and lay the groundwork for the development of secure and resilient technologies as the development progresses through the higher TRL stages. Efforts in this TRL range are characterized by the following key activities:

- Conduct exploratory research—including literature reviews, theoretical studies, and lab experiments—to observe and document the fundamental principles underlying the proposed technology or solution.
- Create initial hypotheses, conceptual models, and key research questions, and identify potential uses and benefits of the technology.
- Formulate basic technology concepts and potential applications based on the observed principles from theoretical and experimental studies.
- Conduct analytical studies and initial laboratory experiments to validate the hypothesis of the proposed technology.
- Identify and document the primary technical challenges, knowledge gaps, and uncertainties that need to be addressed.
- Publish detailed reports, research papers, and presentations to document the key findings and challenges.

### *Key Questions for Each Cyber-Informed Engineering Principle*

#### **Consequence-Focused Design**

How does the proposed research aim to identify dependencies on the digital assets of the proposed concept? What are the assumptions in the concept around interfacing with digital assets?

How does the research effort identify and prioritize potential high-consequence impacts of cyberattacks on critical functions or components?

What opportunities exist for the technology being developed to mitigate the identified cyber-induced, high-consequence impacts during the basic research and theoretical development phase?

What key tasks can be included in the research plan at this stage to continuously identify and mitigate cyber challenges?

### **Engineered Controls**

How does the research effort plan to develop mitigation strategies for cyber-induced, high-consequence events of the proposed concept?

How will the feasibility and effectiveness of the proposed engineered controls be assessed during the basic research and proof-of-concept activities?

Can language for a funding opportunity announcement for the research program encourage collaboration with cybersecurity experts or other industry partners?

### **Secure Information Architecture**

Is there a plan to identify and document assumptions of critical data availability and dependency for the development of a proof of concept for the proposed technology?

What opportunities exist to ensure secure data flows and prevent unauthorized access or manipulation of critical information?

How will the research team validate the efficacy of secure information pathways during proof-of-concept testing and experimentation?

### **Design Simplification**

What theoretical design and engineering hypotheses can be formulated at this stage to simplify the design of the proposed concept to enhance security and resilience?

What opportunities exist for the proposed research to simplify the design or architecture of the concept being developed at this early stage?

What strategies are proposed to prioritize simplicity in design decisions and minimize dependencies on complex digital functionalities during these fundamental research and proof-of-concept phases?

How does the research plan streamline the future development of design to mitigate cyber-induced consequences without compromising functionality or performance?

### **Resilient Layered Defenses**

How is the research plan incorporating resilient defense strategies, such as redundancy and diversity, to provide multiple lines of defense against cyber threats during the early stages of technology development?

What hypotheses can be developed to incorporate effective layers of defense to mitigate potential cyber vulnerabilities and impacts and ensure the resilience of the proposed concept?

Which proposed tasks in the research plan evaluate the effectiveness of layered defense mechanisms through simulations or lab testing during the proof-of-concept phase?

### **Active Defense**

Are there opportunities to identify and explore active defense mechanisms against cyber threats in real time during the basic research and proof-of-concept activities?

How will the proposed concept incorporate dynamic elements to detect, respond to, and neutralize cyberattacks or anomalies? What assumptions are being made about the need for active defense strategies?

Is there a plan to define specific scenarios or use cases that should be simulated to assess the performance and efficacy of active defense measures of the proposed concept?

### **Interdependency Evaluation**

What assumptions are being made about the dependencies of the proposed concept on other digital technologies? How are these assumptions being documented and tracked?

How is the research team assessing and understanding the interdependencies among various system components or operational assets of the proposed concept?

What efforts are included in the research proposal or plan to identify potential cyber challenges introduced by system interdependencies and dependencies on external factors?

How can requirements in funding announcements encourage collaboration with experts from different disciplines or operational departments to evaluate and mitigate cyber vulnerabilities and impacts on the research activities at this stage?

### **Digital Asset Awareness**

How can language in funding announcements impel documentation of assumptions and awareness about digital assets needed for development of proposed concepts and their relationship to high consequence scenarios?

How will the research plan aims to assess and mitigate cyber induced high consequence scenarios leveraging the digital assets, including hardware, firmware, and software components that might be needed for future technology development beyond these initial stages?

What procedures or protocols in the research plan will ensure that digital asset awareness is maintained and updated regularly throughout the initial stage of concept development and lab testing to determine their impacts on mitigating cyber induced high consequence scenarios?

### **Cyber-Secure Supply Chain Controls**

How can the requirements in the funding announcements encourage the development of effective procurement strategies and secure supply chain assessments for the components and materials sourced for the research project?

What are the assumptions around the security and trustworthiness of the supply chain of the software and hardware components needed for the proposed concept? How will they be documented and tracked?

### **Planned Resilience**

How well does the research team understand and document the fail-safe and fail-secure modes of the proposed concept?

How will the research project ensure the resilience and continuity of operations in case of a cyberattack or compromise?

What strategies can anticipate and mitigate the impacts of potential cyber incidents or disruptions on critical functions and components?

How will the research team test and validate the efficacy of the planned resilience strategies of the proposed technology during the proof-of-concept and testing phase?

### **Engineering Information Control**

What are the assumptions about the criticality and sensitivity of engineering information at this early stage of R&D? How are these assumptions documented and tracked?

How is sensitive information—including conceptual design specifications, mathematical formulations, and testing data—being protected from unauthorized access during the project execution?

What information control strategies are being proposed to protect critical engineering information at the early stages while allowing for the publication and dissemination of key findings?

Are there controls and protocols to prevent unauthorized disclosure or misuse? How does the research proposal and data management plan restrict access to engineering information based on role-based permissions and authentication mechanisms?

### **Cybersecurity Culture**

How can federal program managers foster a cybersecurity-aware culture among members and stakeholders involved in the early stages of R&D?

What relevant initiatives or training programs can be identified and implemented to raise awareness about cybersecurity challenges and impacts among researchers, developers, and project collaborators?

Can language in the funding announcement encourage or require cross-domain cybersecurity and related training and collaboration with cyber experts throughout the execution of the research project?

What cybersecurity reporting and tracking requirements should be included in the execution of the research projects to enable a culture of cyber awareness?

### Assessment Metrics for TRLs 1–3: Proof of Concept

- Percentage of critical functionalities identified and analyzed for potential consequences of cyberattacks
- Level of detail in the research plan highlighting the high-consequence cyber vulnerabilities of the proposed technology
- Completeness of digital asset inventory, measured by the percentage of hardware, firmware, and software components tracked
- Frequency of updates to the digital asset inventory to reflect changes in the research project
- Accuracy of vulnerability assessments conducted on digital assets, quantified by the number of vulnerabilities identified and mitigated
- Participation rate in cybersecurity training sessions among project team members
- Number of cybersecurity incidents reported and resolved during the research phase, indicating a proactive approach to cybersecurity
- Level of integration of cybersecurity considerations in project documentation and communications, assessed through document review.

## TRL 4-6: Technology Development to Prototype Demonstration

The research efforts in TRLs 4–6 advance from technology development to prototype demonstration, refining concepts and testing to validate their feasibility in realistic and relevant environments. The efforts at this stage include developing realistic prototypes, exploring and answering integration and adoption challenges in the field, improving the design and performance of the technology prototype, and demonstrations in realistic lab or field environments. Program managers can leverage CIE principles at this higher TRL stage of the prototype demonstration to ensure the development of innovative technologies that can be securely and resiliently integrated and adopted in the field. The activities in this TRL range provide key opportunities for federal program managers to integrate and assess CIE principles in their research portfolios, and they can help federal program managers identify cyber-induced consequences and explore ways of leveraging secure supply chains. The activities in this stage are characterized by the following key activities:

- Develop and validate individual technology components or subsystems in a controlled laboratory setting.
- Create laboratory-scale versions of the components and conduct experiments to verify their performance and usability.
- Test integrated systems to ensure that all components work together as intended and meet the specified performance criteria.
- Develop prototypes that closely represent the final systems or products and validate their performance in a relevant environment.
- Identify potential integration risks and adoption challenges associated with the proposed technology and develop strategies to mitigate them.
- Refine the technical requirements and design specifications based on the results of the validation and testing activities.

### *Key Questions for Each Cyber-Informed Engineering Principle*

#### **Consequence-Focused Design**

How accurately and comprehensively are the key functionalities of the prototype and their cyber dependencies being explored and documented?

How does the project plan aim to validate the accuracy of the cyber-induced, high-consequence events identified for the prototype during the testing and validation phase?

What design and engineering refinements are possible at the prototype stage to either mitigate or eliminate cyber-induced consequences to the critical functionalities of the prototype?

How will the effort identify and evaluate the cyber-induced, high-consequence scenarios during the integration of the prototype in the realistic field environment?

#### **Engineered Controls**

What engineered controls are being integrated into the technology prototype design to mitigate cyber impacts and enhance resilience?

How will the feasibility and effectiveness of the proposed engineered controls be assessed through testing and demonstration activities?

Are there opportunities to collaborate with cybersecurity experts, system integrators and operators, or industry partners to develop engineered control-based mitigations to high-impact cyber consequences? How can funding announcements for research at this stage encourage or require such multidisciplinary collaboration?

### **Secure Information Architecture**

How does the research plan identify and assess the impacts of information flows on the critical functions of the technology prototype?

What architectural controls are being implemented in the development and integration of the technology prototype to ensure secure data transmission, storage, and processing?

What efforts identified in the research plan will validate the efficacy and performance of the information architecture of the prototype through rigorous testing and validation processes during demonstrations?

### **Design Simplification**

How does the proposed research effort plan to identify opportunities to simplify the design to enhance the security and resilience during the prototype development and demonstration stage?

What efforts in the research effort will simplify the design or architecture of the technology prototype to reduce complexity and mitigate adverse cyber-induced impacts?

How will design simplification principles be applied to optimize operational efficiency and minimize cybersecurity impacts during the prototype integration and demonstration in realistic environments?

### **Resilient Layered Defenses**

What are the fail-safe and fail-secure modes of the proposed technology prototype? How accurate is the identification of these modes, and what assumptions are being made regarding the development and integration of the proposed technology prototype?

What opportunities exist in the development and integration of the technology prototype to safeguard the technology from potential cyber vulnerabilities and related impacts?

What efforts are proposed in the research plan to evaluate the effectiveness of the layered defense mechanisms through real-world testing during prototype demonstrations?

### **Active Defense**

What dynamic elements are being incorporated into the technology's design to actively defend against cyber threats and mitigate impacts in real time during the prototype development and demonstration?



How can language in the funding announcement necessitate the identification and deployment of relevant active defense measures for the technology prototype development, testing, and demonstration?

What specific scenarios or use cases are included in the research proposal to assess the performance and efficacy of active defense measures during the protocol integration and demonstration?

### **Interdependency Evaluation**

How does the research plan integrate inputs from multiple disciplines and operational departments to identify the dependencies of the proposed technology prototype on other systems and assets?

What efforts are being made to identify and mitigate cyber-induced, high-consequence events introduced by system interdependencies that could impact the critical functions of the technology?

How can language in the funding announcements and project contracting necessitate collaboration with cyber and other system experts to develop, validate, and demonstrate the proposed technology prototype?

### **Digital Asset Awareness**

How does the project plan address the need to mitigate cyber included high consequence scenarios leveraging the digital assets including leveraging hardware, firmware, and software components throughout the prototype development and demonstration phases?

What measures are in the project execution plan to actively monitor and analyze vulnerabilities within digital assets associated with the technology prototype? How will the mitigations for high consequence scenarios be demonstrated leveraging the digital assets?

What procedures or protocols are being proposed in the project plan to maintain and regularly update digital asset awareness to address evolving cyber vulnerabilities and their impacts on high consequence scenarios?

### **Cyber-Secure Supply Chain Controls**

How does the research project plan incorporate supply chain management practices to ensure the integrity and security of components sourced for the prototype development and demonstration?

How can requirements and compliance language in the funding announcements necessitate the development of measures to verify the trustworthiness and compliance of suppliers and vendors with cybersecurity standards for prototype development and demonstrations?

Do research plans necessitate audits or assessments to evaluate the effectiveness of supply chain controls and mitigate potential disruptions introduced by third-party dependencies during prototype demonstrations?

### **Planned Resilience**

How does the research plan account for developing and demonstrating resilience and continuity of operations for the key functionalities of the technology prototype?

What strategies are being implemented to anticipate and mitigate the impacts of potential cyber incidents or disruptions of critical functions or operations during prototype demonstrations?

Has the research team developed contingency plans or resilience measures to maintain essential functions and services even under adverse cyber conditions?

### **Engineering Information Control**

How is sensitive engineering information—including design specifications, configurations, and testing data—being protected from unauthorized access or disclosure during prototype development, integration, and demonstration?

How can funding announcement language necessitate the need for robust engineering data management plans for the efforts in prototype development and demonstration stages?

Has the research team established controls and protocols to restrict access to engineering information based on permissions and authentication mechanisms?

### **Cybersecurity Culture**

How is the research plan fostering a cybersecurity-aware culture among research team members and stakeholders involved in the prototype development and demonstration?

What initiatives or training programs can be stipulated as part of the funding or contracting requirements for the researchers, collaborators, and technology integrators?

What mechanisms are in place to encourage the proactive reporting of cybersecurity incidents, vulnerabilities, or concerns to promote a culture of continuous improvement?

### **Assessment Metrics for TRL 6: Prototype Demonstration**

- Number of engineered controls implemented in the technology's design, categorized by their effectiveness in mitigating cyber-induced, high-consequence events
- Percentage of engineered controls validated through testing
- Evaluation of the scalability and adaptability of engineered controls to different system configurations and environments
- Depth of interdisciplinary collaboration, measured by the number of departments or disciplines involved in interdependency assessments
- Identification of potential system interdependencies and associated cyber consequences, quantified by the number of identified dependencies and their impact analysis
- Effectiveness of mitigation strategies in addressing interdependencies, assessed through simulation or scenario analysis
- Evaluation of resilience measures against simulated cyberattacks or disruptions during prototype demonstrations.

## TRL 7-9: Prototype Deployment to Commercial Deployment

TRLs 7–9 encompass the final phases when a technology prototype is demonstrated in a real-world operational environment, fully integrated, and assessed through the full range of operational conditions. The activities in this stage include addressing key integration and technical adoption challenges of the technology, market analysis and identification of commercialization pathways, real-world field deployment and demonstration, and gathering feedback from users and stakeholders. During these stages, federal program managers can enforce CIE principles to ensure the secure and resilient transition, adoption, and commercialization of innovative technologies. This approach ensures that the technologies and systems are functional, secure by design, and resilient against potential cyber threats, supporting a smooth transition to widespread deployment and commercialization. Following are the key activities that characterize TRLs 7–9:

- Conduct operational testing and evaluation of a final prototype in the actual operational environment.
- Deploy technology prototype/product in real-world conditions to validate its performance, reliability, and functionality, ensuring it meets all operational requirements.
- Perform extensive testing and demonstration to confirm that the technology performs as expected under all anticipated operating conditions.
- Ensure that the final technology product complies with all relevant regulatory and certification requirements.
- Identify and develop manufacturing processes, scale up production capabilities, establish supply chains, and launch the technology into the market.

### *Key Questions for Each Cyber-Informed Engineering Principle*

#### **Consequence-Focused Design**

How well does the developed technology demonstrate resilience against high-consequence cyberattacks or compromises during real-world testing and integration?

What evidence is provided by the research proposals to validate that critical functionalities have been designed and engineered to mitigate the potential consequences of cyber threats during integration and demonstration?

How comprehensively and accurately has the research team documented the key cyber-induced consequences that are still not mitigated in the final product or prototype?

#### **Engineered Controls**

What engineered controls have been integrated into the technology's design to enhance the security features and mitigate the cyber impacts during the real-world integration and operational testing?

How does the research plan propose to assess the effectiveness of the engineered controls? What rigorous testing and validation activities will be used to evaluate the technology's resilience and mitigations against cyber threats?

How can the language in the funding announcement impel collaboration with cybersecurity experts or industry partners to validate the real-world implementation and effectiveness of engineered control strategies?

### **Secure Information Architecture**

How will the effectiveness of the developed secure information architecture be validated and demonstrated in the real-world operational environment for the developed technology?

What architectural controls are in place to ensure secure data transmission, storage, and processing within the real-world integrated system?

How well are the requirements and assumptions for the criticality of data and secure information architecture documented for future technology integration and adoption?

### **Design Simplification**

How does the research plan evaluate the effectiveness of the design implications to mitigate cyber-induced consequences that are implemented in the final technology prototype?

How well are the assumptions around the design simplification decisions documented during the development of the final technology prototype? How can they be leveraged by future integrators and adopters of the technology?

### **Resilient Layered Defenses**

How are resilient layered defense mechanisms being implemented to provide redundancy and resilience against cyber threats during system integration and operational testing?

What layers of defense have been integrated into the technology's design to safeguard against potential cyber vulnerabilities and related high-consequence impacts on critical functionalities?

What testing and validation plans are being proposed to comprehensively assess and evaluate the effectiveness of the resilient layered defense strategies in the real-world environment?

### **Active Defenses**

What dynamic elements have been incorporated into the technology's design to enable active defense measures against cyber threats in real time during system integration and operational testing?

How well are the assumptions and requirements for the implementation of active defense mechanisms documented for future integrators and adopters of the developed technology?

What is the proposed testing, validation, and demonstration plan for assessing the efficacy of the deployed active defense strategies?

### **Interdependency Evaluation**

How comprehensive and technically sound is the research proposal's evaluation of the interdependencies of the proposed technology with cyber and related digital systems? How well have these been documented to enable secure and resilient field integration and adoption?

How has the research team addressed the cyber vulnerabilities and impacts introduced by the system interdependencies for the developed technologies?

How has input from multiple disciplines and operational departments been integrated to assess and mitigate cyber-induced, high-consequence events introduced by system interdependencies during system integration and operational testing?

How will these interdependencies and related mitigations be validated and demonstrated in real-world field deployment environment?

### **Digital Asset Awareness**

How comprehensive and accurate is the inventory of digital assets being maintained to track hardware, firmware, and software components within the integrated system for the developed technology and their impacts to critical functionalities and high consequence scenarios?

What measures have been adopted in the developed technology to monitor continuously and analyze vulnerabilities within digital assets associated with the final prototype to mitigate high consequence scenarios?

What procedures or protocols should be established to ensure that digital asset awareness is updated and refined regularly along with their relationship to critical technology functions and evolving system integration and adoption challenges?

### **Cyber-Secure Supply Chain Controls**

What supply chain management practices have been implemented to ensure the integrity and security of components and materials sourced for the final technology prototype or product?

What continuous measures are taken to verify the trustworthiness and compliance of suppliers and vendors?

What criteria and assessment mechanisms have been developed to select the appropriate sources for hardware, software, and firmware components for the developed technology? How can this information be shared with future integrators and adopters of the developed technology?

### **Planned Resilience**

How accurate and technically sound are the fail-safe and fail-secure mode identifications for the finally developed technology in a real-world, fully integrated system environment?

What strategies have been implemented to anticipate and mitigate the impacts of potential cyber incidents or disruptions on critical functions for the deployed technology in the field?

What are the cost impacts of the planned resilience measures that are implemented in the final product?

### **Engineering Information Control**

How accurate and comprehensive is the identification of the key sensitive engineering information—including design specifications, configurations, and testing data—that needs to be protected from unauthorized access or disclosure for the final developed and integrated technology?

What measures have been proposed to protect the key engineering information during the field integration, deployment, and demonstration of the developed technology?

### **Cybersecurity Culture**

How is the research project fostering a cybersecurity-aware culture among researchers, integrators, and adopters of the final technology?

What training programs have been identified and developed to raise awareness about cybersecurity best practices and protocols among researchers, developers, and project collaborators?

What awareness and training has been developed to communicate key information about the cybersecurity features and controls of the developed technology that can be leveraged by future adopters and users?

What mechanisms for cyber incident reporting have been developed for users and future adopters to provide information about cybersecurity challenges around the final technology deployed in the field?

### **Assessment Metrics for TRL 9: Commercial Deployment**

- Comprehensiveness and accuracy of the identified cyber-induced, high-consequence scenarios for the final technology
- Effectiveness of the engineered controls deployed in the final technology to mitigate cyber consequences to critical functions and enhance cyber resilience
- Compliance with secure information architecture standards and guidelines, measured against established benchmarks
- Effectiveness of layered defense mechanisms, quantified by their ability to detect, prevent, and mitigate cyber threats in real-world scenarios
- Integration of redundancy and failover mechanisms to enhance system resilience against cyberattacks
- Evaluation of system performance under stress conditions or cyberattacks, comparing expected outcomes with observed results
- Assurance of supply chain integrity, verified through supplier audits and verification of product authenticity
- Implementation of contractual obligations and procurement policies to enforce cybersecurity requirements across the supply chain
- Development and implementation of cyber incident reporting mechanisms for the future adopters and users of the developed technologies.

# Research and Development Guide Development Team

Research and Development Guide development was led by researchers at NREL and INL, with significant review from a multi-stakeholder team and volunteer members of the CIE Community of Practice.

**Richard Macwan**

*National Renewable Energy Laboratory*

**Maurice Martin**

*National Renewable Energy Laboratory*

**Emily Waligoske**

*National Renewable Energy Laboratory*

**Gareth Williams**

*National Renewable Energy Laboratory*

**Virginia Wright**

*Idaho National Laboratory*





