Federal Register Notice: 89 FR 78915, Federal Register :: Networking and Information Technology Research and Development Request for Information on Cyber-Physical Systems Resilience Research, September 26, 2024.

**Request for Information on the National Cyber-Physical Systems Resilience Plan**

Pacific Northwest National Laboratory

Pacific Northwest
NATIONAL LABORATORY

# Response to 89 FR 78915

## Pacific Northwest National Laboratory

October 2024

Thomas Edgar
David Manz
Elena Peterson
Thomas Carroll
Jessica Smith
Marissa Decillis
Veronica Adetola
Michael Henson
Lori Ross O'Neil



U.S. DEPARTMENT OF ENERGY | Prepared for the U.S. Department of Energy under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory (PNNL) has extensive capabilities and experience in cyber-physical security and resilience. We develop integrated security solutions that address both cyber and physical vulnerabilities in critical infrastructure systems like energy, transportation, and water sectors. Engaged in advanced research and development, PNNL works to identify and mitigate emerging riks associated with the convergence of cyber and physical domains and create cutting edge solutions like applying zero trust concepts into operational technology environments and utilizing deception as an easy-to-use industry detection technique. Our specialization in threat analysis and detection involves the use of machine learning and AI to enhance the identification and response to potential attacks.

PNNL is also focused on resilience engineering through investments like the Resilience Through Data-Driven, Intelligently Designed Control (RD2C) Initiative, working to enhance the ability of infrastructure systems to recover quickly and maintain operations following disruptions. Using sophisticated modeling and simulation tools, it is possible assess the impact of cyber-physical threats and test the effectiveness of security measures in controlled environments. The laboratory collaborates with government, industry, and academic partners to develop standards, share best practices, and advance the field of cyber-physical security. Additionally, PNNL offers training and educational programs that prepare organizations and individuals to meet modern cyber-physical security challenges.

## PNNL's Response: A National Plan for Cyber-Physical Systems Resilience

Cyber resilience refers to an organization's ability to continuously deliver the intended outcome, despite adverse cyber events. It encompasses the abilities to anticipate, withstand, recover from, and evolve to improve capabilities against future cyber threats. The most common definitions of cyber resilience generally include the following components:

- Preparation: The capacity to predict and prevent cyber threats. This involves conducting risk assessments, threat modeling, and implementing proactive defense strategies.
- Resistance: The ability to resist and endure when a cyber incident occurs without significant disruption. This includes having strong preventive measures like firewalls, intrusion detection systems, and robust security protocols in place.
- Recovery: The speed and effectiveness with which an organization can recover from a cyber incident. Effective disaster recovery plans, data backup solutions, and incident response teams are critical to this aspect.
- Adaptation: The ability to learn from cyber incidents and evolve to be better prepared for future threats. This includes analyzing incident reports, updating security policies, and investing in continuous training and improvement.

The three commonly used definitions of cyber resilience are from NIST, DoD, and DHS.

## National Institute of Standards and Technology (NIST)[1]

NIST describes cyber resilience as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on information systems. Key Elements of their definition includes anticipate (Forecasting potential threats and vulnerabilities), withstand (Robust measures to prevent and resist attacks), recover (Efficient recovery mechanisms post-incident), adapt (Continuous learning and evolving security practices). The definition focuses on balancing preventive, detective, and

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

corrective controls and emphasizing on a holistic approach encompassing technology, processes, and people.

### Department of Defense (DoD)[1]

The DoD defines cyber resilience as the ability of a system or organization to resist, absorb, recover from, or successfully adapt to adverse occurrences that could cause harm, such as cyber-attacks. Key Elements of their definition includes resisting (Defend against attacks), absorbing (Minimize the impact of attacks), recovering (Restore normal operations swiftly), and adapting (Enhance defenses based on past experiences). The definition has a strong emphasis on mission assurance and operational continuity and incorporates a warfare context in which cyber resilience is crucial to maintaining mission effectiveness under adversarial conditions.

### Department of Homeland Security (DHS)[2]

According to DHS, cyber resilience refers to the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions due to deliberate attacks, accidents, or naturally occurring threats or incidents. Key Elements of their definition includes preparing (Strategic planning and readiness), adapting (Flexibility to handle evolving threats), withstanding (Measures to resist damage), and recovering (Rapid restoration of services). The definition includes a broader scope including deliberate, accidental, and natural disruptions, emphasizes critical infrastructure protection and public-private partnerships and focuses on national security and public safety.

These definitions stress preparation, resistance, recovery, and adaptation as key elements. Each emphasizes the importance of minimizing disruption to crucial services or operations. Overall, cyber resilience strives to ensure the operational continuity and security of an organization's critical services in the face of ongoing cyber challenges and enhancing the ability to develop better defenses.

Digital systems resilience can be robustly achieved through a synergistic approach encompassing both strategic planning and tactical operations. From a strategic perspective, resilience begins with the intentional design and configuration of digital systems to possess inherent resilient attributes. This involves developing more distributed, fault-tolerant system architectures that eliminate single points of failure and ensure continuity of service. Integrating Zero Trust principles into these systems—where no entity is trusted by default—further solidifies the security posture by meticulously managing access controls and continuously verifying every request. Understanding and documenting the base vulnerability states of these systems through comprehensive risk assessments and vulnerability scans is also crucial. Such foundational knowledge enables organizations to anticipate and mitigate potential threats before they materialize, fundamentally strengthening the resilience of the digital infrastructure.

On the tactical and operational front, resilience is further ensured by actively monitoring and responding to threat activities through proactive and adaptive defenses. This involves the deployment of advanced monitoring tools and systems that provide real-time visibility into network activities, detect anomalies, and identify potential security incidents. Proactive defense mechanisms, such as threat intelligence-driven deceptions and automated incident detection and response systems, are essential in identifying and neutralizing threats before they cause significant damage. Adaptive defenses, which dynamically adjust to evolving threats, ensure that security measures remain effective in the face of new and sophisticated attack techniques. By coupling these advanced controls with continuous performance measurement and monitoring, organizations can not only respond to threats more efficiently but also iteratively improve their

[1] https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/302040p.pdf
[2] https://www.dhs.gov/publication/2010-risk-lexicon

resilience strategies. This dual approach of strategic planning and tactical execution creates a resilient digital ecosystem capable of withstanding, recovering from, and adapting to an array of adverse conditions and cyber threats.
A resilient response is multifaceted, achieved by integrating resilience across various layers of an organization's infrastructure. These layers include supply chain, control system design and operation, communication network design and operation, and operator response support.

## Resilience through Supply Chain

Supply chain resilience is a critical component of an overall cyber resilience strategy. It involves ensuring the integrity, security, and robustness of all components and services essential for operations. By integrating resilience into the supply chain, organizations can better prepare for and mitigate disruptions, whether caused by cyber-attacks, natural disasters, or other adverse events. Key activities in this regard include collecting comprehensive build materials, tracking vulnerabilities, and establishing a national vulnerability notification system. Here's a detailed overview:

### *1. Collecting Bills of Material for Software, Hardware, and Firmware*

A Bill of Materials (BoM) is a detailed list of all components, including software, hardware, and firmware, used in an organization's IT infrastructure. Enables precise tracking of components and their interdependencies. Facilitates efficient vulnerability management and patching processes. Enhances transparency and accountability in the supply chain.

Strategic Activities:

- Inventory Management: Maintain an up-to-date inventory of all components along with their versions, manufacturers, and dependencies.
- Automated Tools: Employ automated tools to scan and document all software libraries, hardware parts, and firmware versions.
- Supplier Collaboration: Work closely with suppliers to obtain accurate and comprehensive BoMs for all products.

### *2. Tracking and Mapping Vulnerabilities*

Continuously monitoring and identifying vulnerabilities in software, hardware, and firmware components is crucial for proactive defense. Reduces the attack surface by proactively addressing vulnerabilities. It is not currently possible for cyber-physical system operators to determine their full cyber risk exposure for the equipment they have procured and operate. Creating a method and framework to better inform operators how newly discovered vulnerabilities relate to their operations helps them more quickly mitigate the problem, reducing the window for threat exploitation.

Strategic Activities:

- Vulnerability Databases: Utilize databases like NIST's National Vulnerability Database (NVD) to stay informed about known vulnerabilities.
- Automated Scanning: Implement automated vulnerability scanning tools to identify and assess vulnerabilities in real-time.
- Risk Assessment: Conduct regular risk assessments to prioritize vulnerabilities based on their potential impact and likelihood of exploitation.
- Patch Management: Develop and enforce a robust patch management process to promptly address and mitigate identified vulnerabilities.

*3. Creating a National Vulnerability Notification System*

Establishing a centralized system at the national level to inform organizations about new vulnerabilities and their potential impact on their environments. Provides organizations with timely and relevant information to address vulnerabilities. Enhances national cybersecurity posture by ensuring widespread awareness and coordinated response to emerging threats. Reduces the likelihood of widespread exploitation of vulnerabilities by enabling proactive defenses.

Strategic Activities:

- Centralized Repository: Create a national repository that aggregates vulnerability data from various trusted sources.
- Real-Time Alerts: Develop a system to disseminate real-time alerts and notifications about new vulnerabilities to relevant stakeholders.
- User Registration: Allow organizations to register and specify their environments so they receive tailored notifications based on their specific configurations.
- Collaboration and Coordination: Facilitate collaboration between government agencies, private sector entities, and security researchers to enrich the repository with comprehensive, timely information.

## Resilience through Control

Ensuring resilience through control design and operation is crucial for maintaining the functionality and security of critical infrastructure systems, even in the face of cyber threats. This strategy focuses on designing systems with resilience, using simulations to understand risks, implementing new control frameworks for distributed infrastructure, and developing metrics to enhance resilience management. Key elements of the strategy include:

*1. Resilience by Design Using Simulations*

Designing systems with resilience from the start and using simulations to understand cyber risks, identify weaknesses, and optimize control frameworks and mitigation strategies. Provides a proactive approach to cybersecurity by understanding and addressing potential risks before they materialize. Optimizes resource allocation by identifying the most effective controls and mitigations. Enhances the robustness and reliability of control systems.

Strategic Activities:

- Threat Modeling: Develop threat models to identify potential attack vectors and vulnerabilities.
- Co-Simulation Tools: Utilize advanced simulation tools to simulate cyber-attacks and their impact on systems. Exploring across both cyber and physical models is crucial to understanding and evaluating the emergent behavior and risks as the two become increasing intertwined. Co-simulation and integrated modeling tools are crucial to answer the pressing and upcoming securing questions.
- Scenario Analysis: Conduct scenario-based analyses to evaluate the effectiveness of different control frameworks and mitigation strategies. It is important to understand both the highest risk/probable threat scenarios against an existing system and the most reoccurring targets that cause physical impacts to better inform decision makers on how and where to prioritize resilient planning.
- Optimal Control Selection: Use co-design approaches with simulation results to select optimal control frameworks and cyber mitigations tailored to specific risks and operational requirements. Since

resources are limited, it is crucial to create tools that help asset owners prioritize and optimize investments for maximum risk mitigation benefit.

*2. Implementing New Control Frameworks for Distributed Infrastructure*

Adopting and implementing control frameworks and approaches that cater to the more distributed nature of modern critical infrastructure systems. Increases system resilience by reducing single points of failure. Enhances the ability to localize and contain disruptions. Supports scalability and flexibility in managing critical infrastructure.

Strategic Activities:

- Decentralized Control Systems: Develop and implement decentralized control systems that can operate independently and collaboratively.
- Distributed Architecture: Design systems with a distributed architecture to enhance redundancy and fault tolerance.
- Edge Computing: Utilize edge computing to process data locally, reducing reliance on centralized systems and improving response times.

*3. Cyber Attack-Aware Systems Designed to Fight Through Adverse Conditions*

Developing systems that are aware of cyber-attacks and designed to continue operating effectively during and after adverse conditions. Ensures continuity of critical operations during cyber incidents. Reduces the impact of attacks by containing and mitigating them swiftly. Enhances the overall security posture by being prepared for various attack scenarios. Note: this is not the same as threat-aware and indeed can be threat agnostic.

Strategic Activities:

- Intrusion Detection and Response: Implement advanced intrusion detection and response mechanisms to mitigate cyber-attacks in real-time.
- Adaptive Defense Mechanisms: Develop adaptive defense mechanisms that can adjust to evolving threats and conditions dynamically.
- Resilient Communication Protocols: Utilize resilient communication protocols to maintain integrity and availability even under attack.

*4. Creation of New Metrics and Measures for Resilient Response*

Developing new metrics and measures to better understand, monitor, and control resilient responses in real-time. Current metrics are commonly in terms of reliability and robustness and not well suited for resilience. Additionally, metrics in the cyber space are challenging to map to resilience and current risk. New metrics and measures specifically for tracking and driving resilience is necessary to provide quantifiable data to assess and improve resilience practices, enhance situational awareness, and decision-making during cyber incidents, and facilitate continuous improvement and adaptation of resilience strategies. This will need to better address the social and human elements of cyber-physical systems.

Strategic Activities:

- Resilience Metrics: Establish resilience metrics that quantify the ability to anticipate, withstand, recover, and adapt to cyber threats.

- Continuous Monitoring: Implement continuous monitoring systems to track resilience metrics and provide real-time insights into system health and security.
- Incident Reporting: Develop standardized incident reporting frameworks to capture and analyze data on cyber incidents and responses.
- Benchmarking and Improvement: Use resilience metrics to benchmark against industry standards and identify areas for improvement.

## Resilience through Communication Network Design and Operation

Resilience in communication network design and operation is vital for ensuring the continuous delivery of critical services and for enabling robust responses to cyber threats. This strategy involves identifying mission-critical dependencies, implementing proactive and adaptive defense mechanisms, applying Zero Trust principles, and integrating advanced communication technologies like 5G into cyber-physical systems. The key elements of the strategy include the following recommended activities:

### *1. Discovering and Understanding Mission-Critical Cyber Dependencies*

Identifying and understanding the cyber dependencies that are critical for mission success is the first step in enhancing network resilience. Provides a clear understanding of what needs to be protected. Helps prioritize resources and efforts toward safeguarding the most critical elements. Enhances situational awareness and preparedness.

Strategic Activities:

- Dependency Mapping: Create a comprehensive map of all mission-critical systems, networks, and interdependencies.
- Tools for Cyber and Physical Risk Assessment: Physical threats and cyber threats are commonly evaluated independently but real-world threats can and do leverage capabilities from both spaces. Tools to enable analysis across both the physical process and security and cyber security.
- Data Flow Analysis: Analyze data flows to understand how information moves through the network and identify critical nodes and communication paths.
- Stakeholder Engagement: Engage with key stakeholders to ensure a thorough understanding of operational requirements and dependencies.

### *2. Using Proactive and Adaptive Cyber Defense Mechanisms*

Implementing defense mechanisms that can proactively detect and respond to threats based on real-time threat intelligence. Enabling this strategy would enhance the ability to detect and respond to threats in real-time, reduce the dwell time of attackers within the network and provide valuable insights into attacker tactics, techniques, and procedures (TTPs).

Strategic Activities:

- Stronger Threat Intelligence Integration with Tools: Incorporate real-time threat intelligence feeds to inform and update defense strategies. Threat intelligence is a valuable source, but critical infrastructure asset owners often lack the resources to fully utilize it. Integrating these data feeds into more automated tools will alleviate the barrier to entry owner/operators and enable them to benefit from current knowledge of ongoing threat campaigns.

- Deception Technologies as a low barrier to entry defense tool: Use deception technologies to create fake assets and environments that can mislead and trap attackers. Asset owners are often hesitant to deploy new security solutions because of the potential or perceived risks. Deception techniques have low risk of impacting operations and have low false positive rates of detecting unauthorized activities.
- Anomaly Detection: Implement systems to detect abnormal behavior that may indicate a potential attack. The physical process side of cyber-physical systems provides an opportunity to ground and constrain abnormalities in cyber data to help with the base rate fallacy challenge of traditional cyber data.
- Automated Response: Develop automated response mechanisms that neutralize threats and adapt to evolving attack patterns. This can cover the range of automated, autonomic, or even autonomous response with human oversight as needed.

*3. Limiting Attack Impact with Zero Trust Concepts in OT Environments*

Applying Zero Trust principles to Operational Technology (OT) environments to minimize the risk and impact of cyber-attacks. Through the appropriate application of zero trust concepts, it is possible to significantly reduce the attack surface by limiting unauthorized access, contain and minimize the impact of breaches, and provide enhanced visibility and control over the network. If usability is considered in this approach the fears of OT operators can be overcome and enable connectivity, they aspire to create such as access to OT data in business systems while also improving overall security posture.

Strategic Activities:

- Micro-Segmentation: Isolate network segments to limit the spread of attacks.
- Integration of host and network policy and control: Combining host/application sandboxing with network segmentation for full end-to-end data movement mediation and authorization.
- Continuous Monitoring: Continuously monitor all activities within the network to detect and respond to malicious actions.
- Framework across on-prem and cloud assets: Develop approaches and architectures to securely utilize cloud services in OT to prepare for the increasing reliance on cloud applications and infrastructure.

*4. Integrating Cutting-edge Communication Technologies such as 5G into Cyber-Physical Systems*

Leveraging advanced technologies like 5G/ Next-Gen to enhances cyber-physical systems capabilities and mitigates associated risks. Through advanced wireless utilization the capabilities and performance of cyber-physical systems can be enhanced to provide greater flexibility and scalability for network operations. It can also enable new use cases and applications that were not possible with previous communication technologies like enabling more localized and peer-to-peer communication in support of more distributed and isolated operation.

Strategic Activities:

- Benefits Analysis: Evaluate the potential benefits of 5G, including higher speeds, lower latency, mobile edge computing, and greater device connectivity.
- Risk Assessment: Assess the security risks associated with 5G, such as new attack vectors and increased complexity. This includes the 5G network and/or the devices connected to the network.
- Secure Integration: Develop strategies to securely integrate 5G technology into cyber-physical systems, considering aspects like encryption, authentication, and secure configurations.

- Pilot Programs: Conduct pilot programs to test and refine the integration of 5G in controlled environments before full-scale deployment.
- Collaboration with Providers: Work closely with 5G service providers to ensure that security measures are robust and align with operational requirements.

## Resilience through Operator Response Support

Resilience in operator and responder support is essential for maintaining robust defenses and swift responses to cyber threats, particularly in cyber-physical systems. This strategy includes comprehensive training exercises, the development of advanced tools for system emulation and data analysis, and a framework for integrating human decision-making with autonomous control systems, all while promoting collaboration with industry stakeholders. The key elements of the strategy are:

### *1. Resilience by Training and Preparedness Exercises*

Conducting regular training exercises to prepare operators and responders for realistic cyber-attack scenarios. Enhances the readiness of operators and responders to manage actual cyber incidents. Identifies gaps in the current response plans and allows for continuous improvement. Builds confidence and competence in handling cyber threats.

Strategic Activities:

- Simulated Cyber Attacks Exercises: Use high-fidelity simulations and emulations of cyber-physical environments to create realistic attack scenarios. Continuing the investment in programs like DHS CELR or DOE GridEx provides unique and valuable experience to practice and discover the gaps in current resilient response plans. Ongoing support and expansion of these and other like programs is important to make sure the nation's critical infrastructure force is ready to implement resilience measures when necessary.
- Create advanced simulated exercise environment tools to increase the reality of capabilities: In support of the above, continued development of emulation and testbed capabilities for cyber-physical systems is important. This includes developing new models and scenarios, along with the necessary infrastructure and tools, to make training and experimentation environments efficient and high-fidelity.
- Develop TTP test creation pipeline: Threat intelligence continually generates new advisories and CVE reports which are currently not easily operationalized. Develop standards and processes for generating executable TTPs that can be used by industry to validate if their defenses can detect and respond to TTPs detecting in their systems as well as can be used in the training and preparedness exercises to make sure participants are seeing the evolving and most relevant behaviors in the wild.
- National Data Repository of Useful Datasets: The availability of useful datasets has been, and continues to be, a challenge for the research and development industry. Creating national repositories to curate and host high-quality datasets is important to tackle this challenge. National laboratories are the perfect independent broker for such activities to provide the trust to industry to share real datasets but also as a place to generate realistic benchtop/synthetic datasets to fill the repository. Continued support is necessary to address the longitudinal challenge of cyber security where the cyber space and threats evolve rapidly, and aging datasets become less relevant and applicable.

### *2. Developing Tools for Cyber-Physical System Emulation*

Create tools that support efficient and high-fidelity operation of cyber-physical system environment emulation. Provides a safe and controlled environment to test and refine response strategies. Enhances the understanding of how cyber-physical systems react under attack conditions. Supports the development of more resilient system configurations and defense mechanisms.

Strategic Activities:

- Emulation and Experimentation Platforms: Develop advanced emulation platforms that accurately replicate the operational environment of cyber-physical systems. Current capabilities across the national complex can model within specific sectors of critical infrastructure. Expanding and enabling cross-sector and high scale environments are important to enable the research and exercises to optimally prepare for the inevitable future cyber-attacks.
- Scenario Libraries: Build comprehensive libraries of attack scenarios and system responses to test various conditions and threats. Some sectors, such as the power industry, already excel at developing prototypical modeled environments to support research and development. Investments to build out similar capabilities across all the critical infrastructure is important. Also, standardizing modeling languages and protocols will enable sharing off test environments to tackle the reproducibility challenge in research and enable supporting the demand of exercises.
- Integration with Training Programs: Use these emulation tools in training exercises to provide realistic and immersive experiences for operators.

*3. Enhancing Analyst Efficiency through AI/ML*

Developing tools to make analysts more effective and efficient in parsing, understanding, and responding to cyber-physical data and potential attacks using AI/ML advancements. Increases the speed and accuracy of threat detection and response. Reduces the workload on human analysts by automating routine and complex tasks. Enhances situational awareness and decision-making capabilities.

Strategic Activities:

- AI/ML Integration: Research and development in AI/ML approaches applied to cyber-physical specific use cases. This strategy includes efforts to help guide research around promising and inappropriate applications of AI/ML. There is a lot of misinformation on what AI/ML is capable of and the domains around which it is effective. Providing national guidance documents like those that have been developed for other hot topics like block chain[1] would help reduce the wasted investments and effort. Continued human machine teaming research is needed for specific cyber defense uses.
- Automated Threat Prediction and Detection: Develop AI/ML-driven tools to automatically predict, detect and categorize potential threats and anomalies.
- Analysis Decision Support Systems: Create intelligent decision support systems that provide actionable insights and recommendations to analysts. Use LLM advancements to lower the technical barrier to entry for industry engineers to protect their systems. Create data fusion and blending capabilities to bring together the multiple cyber, physical, and business data to provide a holistic real time system understanding.
- Workforce Development: Cross-train cybersecurity and AI experts to foster collaboration and help bring together a common understanding between the two domain experts.

[1] https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf

- Information Sharing: Create a for sharing information on the safety and security of cyber-physical systems that employ AI technologies. (Along the lines of the National Critical Infrastructure Observatory outlined by the President's Council of Advisors on Science and Technology.[1])

*4. Integrating Human Decisions with Autonomous Control Systems*

Developing a framework for when and how human decisions appropriately integrate with new distributed and autonomous control systems. Ensures a balanced integration of human intuition and machine precision in decision-making. Enhances the resilience and effectiveness of control systems through coordinated efforts. Provides flexibility to adapt to different types of cyber threats and scenarios.

Strategic Activities:

- Decision-Making Protocols: Establish clear protocols that define the roles and responsibilities of human operators and autonomous systems. These definitions become increasingly important as proactive and adaptive mitigations and distributed control becomes deployed.
- Human-Machine Interfaces: Develop intuitive interfaces for seamless interaction between human operators and automated systems. Current HMI systems rely on the user to interpret the data and determine intent. New human-machine teaming models are required for systems making decisions independent of operators, ensuring the human remains updated and aware of necessary information using new HMI capabilities.
- Adaptive Decision Frameworks: Implement adaptive frameworks where human and machine decision-making processes are dynamically adjusted based on the context and severity of the situation. Expecting a human to take over in extreme edge cases is unreasonable if the human isn't involved throughout the process. Creating the frameworks on when and how to hand over system control is needed.

*5. Industry Collaboration and Integration*

Ensure that industry is involved and integrated as advisors and collaborators at every step of the national strategy. Leverages industry expertise and innovation to enhance national resilience efforts. Promotes the adoption of best practices and standards across different sectors. Ensures the alignment of national resilience strategies with real-world needs and challenges. Private industry does not bear responsibility for national resilience and security, but they are currently bearing the costs. We need to move beyond talking and into the realm of action and joint developments.

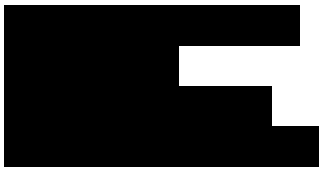
Strategic Activities:

- Public-Private Partnerships: Foster collaborations between government agencies, private sector entities, and academic institutions.
- Industry Advisory Boards: Create advisory boards composed of industry experts to provide insights and guidance on resilience strategies.
- Joint Research Initiatives: Support joint research and development initiatives to advance cybersecurity practices and technologies.

---

[1] President's Council of Advisors on Science and Technology, Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World (Washington, DC: Executive Office of the President, 2024), www.whitehouse.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf.

# Pacific Northwest National Laboratory



*www.pnnl.gov*