MITRE's Response to the NSTC RFI on Cyber-Physical Research

October 25, 2024

For additional information about this response, please contact:

Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

"This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in the National Cyber-Physical Systems Resilience R&D Strategic Plan and associated documents without attribution."

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs), participate in public-private partnerships across national security and civilian agency missions, and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's ~10,000 employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry—allowing MITRE's efforts to be truly objective and data-driven. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision making, technical findings, or policy recommendations.

MITRE's extensive experience in cyber-physical research is rooted in its unique position as a trusted advisor to the government, enabling the organization to address complex challenges in cyber resilience and security. MITRE's work in this domain includes developing advanced analytics and prototype solutions that enhance both cyber defense and offense capabilities. By leveraging its expertise in areas such as machine learning, operations research, and game theory, MITRE has made significant strides in understanding and mitigating cyber threats to critical infrastructure, including transportation systems and military networks.

MITRE's approach emphasizes integrating cyber and physical systems to create resilient and secure environments. This includes applying models to identify vulnerabilities and unifying cyber and electronic operations. MITRE demonstrates its commitment to advancing the state of the art in cyber-physical systems through collaboration with government, industry, and academia, ensuring that solutions are both innovative and practical. Operating without commercial or political pressures, MITRE provides objective, data-driven insights critical to shaping national cyber-physical research strategies.

Overarching Recommendations

Building on MITRE's extensive experience and commitment to addressing complex national challenges, we present a set of overarching recommendations designed to enhance the resilience and security of cyber-physical systems. These recommendations aim to integrate innovative research, foster collaboration, and drive strategic advancements across sectors. By focusing on resilience by design, predictive defense technologies, and cross-sector partnerships, we can develop comprehensive strategies that safeguard critical infrastructure and ensure a safer, more secure future.

Integrate Cyber-Physical Security into a Unified Research Framework. Integrating cyber-physical security into a unified research framework is essential for addressing the complex threats facing critical infrastructure. By combining cybersecurity, physical security, and operational resilience, the nation can develop comprehensive protection strategies that address vulnerabilities across all dimensions. This approach fosters collaboration between experts,

creating holistic solutions that anticipate and mitigate a wide range of threats. Research should focus on advanced threat detection and response mechanisms that operate seamlessly across domains, leveraging technologies like artificial intelligence (AI) and machine learning (ML). This integrated framework will inform the development of cohesive security strategies, ensuring robust protection against evolving threats.

Focus on Resilience, Composability, and Secure Design. Encourage research and development (R&D) initiatives that embed resilience principles into the design and operational phases of cyber-physical systems. Research should explore adaptive and composable systems capable of recovery across various threat scenarios. Additionally, ensure that systems-of-systems are secure by design, promoting integrated and holistic security measures throughout their lifecycle.

Advance Research in Predictive and Proactive Defense Technologies. Support research into AI, ML, and advanced modeling and simulation to enhance predictive threat analysis and real-time response capabilities. These technologies can significantly improve system resilience.

Foster Cross-Sector Research Collaboration. Encourage collaborative research efforts between government, industry, and academia to share insights and innovations. This collaboration will drive the development of resilient systems and enhance the nation's collective security posture.

Integrate Public Perceptions into Resilience Strategies. A recent MITRE-Harris poll[1] reveals that while the American public recognizes the critical role of infrastructure security, there are significant concerns about recovery capabilities and differing views on responsibility. With 29% believing recovery is solely a federal duty and 49% seeing it as a shared responsibility among various government levels and private operators, these perceptions are crucial for national-level planning. By incorporating public expectations into the national cyber-physical research strategy, we can build trust and cooperation, ensuring policies are both technically robust and socially supported. This alignment is vital for effective implementation and public buy-in, ultimately enhancing national resilience and security.

Inputs Requested in RFI

1. Threat-agnostic approaches for resilience are of special interest. As part of the input, we are primarily concerned with the ability of cyber-physical systems to recover and adapt while ability to withstand may be already covered in the current risk assessment and management efforts. We are particularly interested in how resilience by design or resilience by intervention can prepare for recovery and adaptation in different threat scenarios as well as in threat-agnostic situations.

Develop and Direct Research Initiatives to Establish Clear Metrics for Assessing and Prioritizing the Resilience of Cyber-Physical Systems (CPS). This research should focus on defining key performance indicators that measure system robustness, adaptability, and recovery time, providing a common framework for evaluating and enhancing the security and reliability of

[1] MITRE-Harris Poll Finds U.S. Public Is Worried about the Security of Our Critical Infrastructure. 2024. MITRE, https://www.mitre.org/news-insights/news-release/mitre-harris-poll-finds-us-public-worried-about-security-our-critical, last accessed October 15, 2024.

critical infrastructure. By creating a standardized approach to operationally prioritize, test, and evaluate CPS survivability, these metrics will not only guide the design of more resilient systems but also inform discussions on the relative resiliency of existing technologies, ultimately leading to improved strategies for mitigating disruptions.

Enhance Data Integration for Real-Time Modeling and Simulation. To maximize the effectiveness of modeling and simulation (M&S) in cyber threat intelligence, research should aim to improve the integration of high-quality, real-world, and real-time data into simulation environments. This includes developing methods to seamlessly incorporate diverse data sources, ensuring simulations accurately reflect current system states and potential adversary actions. By encompassing multi-domain threat modeling, such as large-scale cyber attacks following significant weather events, enhanced data integration will lead to more precise analyses, enabling better-informed decisions and improved system resilience.

Establish Methods for Prioritizing Investments into Resilient Cyber-Physical Systems. Research should focus on expanding the impact of design principles that integrate security considerations early in the development of CPS, such as Cyber-informed Engineering, Secure by Design, and Zero Trust architectures. By adopting a mindset that assumes systems are compromised, engineers can implement redundancy, diversity, and failsafes to limit the impact of cyber attacks. However, implementation of these principles after systems have been designed or deployed remains prohibitively expensive in many cases. Instead, research should focus on developing strategies and methods to prioritize security enhancements and mitigation techniques. Prioritization should consider threat actor capabilities, intent, and future growth *in addition* to the impact or consequence of a cyber-induced adverse event. This proactive, but threat-actor-agnostic, approach will enhance system resilience, making it more difficult for adversaries to exploit vulnerabilities, especially as emerging technologies like AI and ML are increasingly adopted.

Conduct Research to Evaluate and Streamline Security Regulations for Critical Infrastructure. Research should focus on evaluating the effectiveness of current security regulations and identifying outdated or ineffective requirements. This involves developing methodologies to assess regulatory impact and streamline guidance to align with modern threat landscapes. By reducing unnecessary burdens, this research will help critical infrastructure operators optimize resource allocation and enhance overall security posture.

Recommend Best Practices for Operational Continuity and Resilience. To enhance coverage against cyber threats, weather events, and system failures, research should focus on developing best practices for operational continuity and resilience. This involves identifying strategies for redundant monitoring, manual overrides, and built-in safety thresholds, particularly in remote management systems like Industrial Control Systems (ICS). By addressing these areas, we can mitigate impacts and ensure robust protection for cyber-physical systems, reducing vulnerabilities and enhancing overall system resilience.

2. Examples of domains and application of interest include but are not limited to critical infrastructure and systems for energy, transportation, medical, agriculture, water, space, manufacturing, and other R&D topic areas in which the strategic plan should focus, as well as details that should be considered when/if the topic area is elaborated in the strategic plan.

Align Research Along CISA's National Critical Functions. Aligning this cyber-physical research strategy with DHS/CISA's National Critical Functions (NCFs) is strategically beneficial and represents sound policy. The ongoing cataloging and updating of the NCFs allows for prioritized response and risk management, evolving from an entity-driven approach to one focused on functional outcomes. This alignment ensures endeavors are integrative, maximizing impact across sectors.

- **Understanding Interdependencies and Risks**: The complex interdependencies within and across U.S. critical infrastructure heighten the risks to continuous operation of the NCFs. Recognizing these interdependencies is essential for effective prioritization and risk management.
- **Strategic Risk Management**: The NCF set is organized into four areas: Connections, Distribution, Management, and Supplies. While risk management has progressed beyond entity-driven hardening, national-level impacts can still arise from cascading system-level threats, such as sophisticated cyber attacks, CPS compromise, natural disasters, or systemic failures. Further expanding tool capabilities and conducting advanced tabletop exercises will facilitate broader understanding of the interconnectedness, strengths, and weak spots of the NCF areas.
- **Innovative Approaches and Tools**: Expanding NCF area-level actions and cross-area strategies represents the next evolution of risk management. The STAR (Suite of Tools for the Analysis of Risk), hosted on CISA's Mission Critical Test Environment (MCTE), connects the 55 NCFs to assets, sectors, and responsible owners, with STAR v2 enhancing capabilities through advanced tools and datasets. MITRE can leverage numerous existing and future studies, datasets, and technologies to continue building on the early foundation of STAR.

Incorporate New Risk Mitigation Strategies:

- **Avoidance and Mitigation**: Risks can be avoided, mitigated, transferred, or accepted, but effective management requires a comprehensive understanding of threat scenarios. While individual risks may be inevitable, we must proactively address potential cascading failures. Doing so may require new real-time operational models, dashboards, and reporting mechanisms.
- **Decoupling and Autonomy**: Eliminating risks involves decoupling critical systems or enabling continuous operation through technological innovations, such as autonomous systems with AI-enhanced offline control. Digital twinning and enhancing localized capabilities can be researched and validated.
- **Real-Time Mitigation**: Implementing near-real-time stop-gap actions to control problems and enhance human decision making is crucial. Exploring extensible control mechanisms across disparate systems can enhance resilience. This will require new modeling, data categorization, and reporting across multiple sectors.

- **Risk Sharing**: Increasing interconnectedness through actionable intelligence and legal protections can enhance redundancy and defense-in-depth, allowing for flexible emergency functions across technologies and networks.

These strategies should be explored through technical studies, detailed modeling, and pilots to enhance and/or complement the STAR program. Grounding the research strategy in CISA's framework ensures a robust approach to safeguarding critical infrastructure, making it essential for a comprehensive national strategy.

Innovate Tools for Dynamic Attack Surface Management in Critical Infrastructure. As critical infrastructure becomes increasingly digital and interconnected, managing the attack surface is essential to minimizing vulnerabilities. Research should aim to develop advanced tools and methodologies that dynamically assess and reduce the attack surface, balancing the need for operational visibility with security. By innovating in this area, we can better protect infrastructure from cyber threats while maintaining the efficiency and effectiveness of operations.

Develop High-Fidelity Modeling and Simulation Frameworks for Critical Infrastructure. Research should focus on creating advanced M&S frameworks that leverage digital twin technology and virtualization to provide realistic environments for testing and evaluation of critical infrastructure systems. These frameworks can help asset owners and operators understand vulnerabilities and optimize resource allocation for security. By reducing costs and improving accessibility, these M&S tools can enhance decision making and resilience at both regional and national levels.

Additional Examples of Domains and Applications of Interest (Non-exhaustive):

- **Smart Transportation, Autonomous Vehicles, Vehicle-to-Infrastructure (V2X) Security**: Secure, safe, and resilient transportation infrastructure is critical to the world economy. Vehicle cybersecurity still needs improvement, and relatively little focus has been placed on ensuring the overall transportation infrastructure is resilient. The vehicle community has largely relied on manufacturers to set and meet their own security standards, and is often limited by lack of data on realistic threats and resilience metrics. In addition, vehicle manufacturers are not modeling the V2X environment or self-nominating security requirements to ensure the overall infrastructure is secure.
- **Energy Infrastructure**: Secure and resilient energy infrastructure is vital for economic stability and national security. The power grid faces increasing cyber threats, yet there is a need for more comprehensive frameworks to enhance its resilience. The energy sector often lacks real-time threat detection and response capabilities, which are crucial for preventing disruptions. Additionally, there is insufficient data on potential threats, resilience metrics, and dynamic interdependencies on the sector, limiting the ability to model and mitigate risks effectively. Collaborative efforts between stakeholders are essential to establish robust security standards and ensure the grid's integrity.
- **Medical Devices and Healthcare Systems**: The cybersecurity of medical devices and healthcare systems is critical to patient safety and data protection. As connectivity increases, these systems become more vulnerable to cyber threats. The healthcare community often relies on manufacturers to self-regulate security standards, which can lead to inconsistencies. There is a pressing need for comprehensive guidelines that address authentication, data encryption, and regular security updates. Ensuring the security of

medical devices, systems, and networks requires a coordinated approach to protect sensitive patient data and maintain device functionality.

- **Water Systems**: Protecting water supply systems from cyber threats is essential for public health and safety. Water treatment facilities and distribution networks are increasingly targeted, yet there are continued inconsistencies in the implementation of security practices and standards. The water sector often struggles with risk assessment and incident response capabilities, which are crucial for safeguarding against potential attacks. Developing robust security measures and conducting regular vulnerability assessments are necessary to ensure the integrity and reliability of water systems.
- **Space Systems**: The security of space systems is critical as reliance on satellites for communication and navigation grows. Space assets face unique cyber and physical threats, yet there is limited focus on comprehensive protection strategies. The space industry also provides additive and alternate communication paths for numerous critical functions and thus requires additional risk mitigation strategies and enhanced security measures for the transport of sensitive data. Collaborative efforts are needed to develop strategies that protect these assets, ensuring the reliability and continuity of space-based services.
- **Manufacturing**: Manufacturing processes depend heavily on ICS, which are susceptible to cyber-physical threats. The sector often lacks consistent implementation of security best practices, industry standards, and cybersecurity maturity models to measure against, leaving ICS vulnerable to attacks that can disrupt production. There is a need for best practices in network segmentation, access control, and incident response to protect manufacturing operations. Establishing comprehensive security standards and conducting regular assessments are crucial for safeguarding the integrity of manufacturing systems.

3. Other Inputs. (This RFI seeks input to shape a whole-of-government effort on research and development that will strengthen cyber-physical resilience. In the context of this RFI, we refer to threats to include cybersecurity, physical, natural disasters including extreme weather events or other hazards such as earthquakes, and the potential for adversary use of AI to disrupt systems as well as deceive human operators of critical infrastructure systems.)

Further Consider the PCAST Recommendation for a National Critical Infrastructure Observatory. We encourage further consideration of the President's Council of Advisors on Science and Technology (PCAST) recommendation[2] to establish a National Critical Infrastructure Observatory aimed at enhancing resilience across U.S. critical infrastructure. This observatory would serve as a "lived-in" testbed for real-world applications, focusing on a range of threats, including natural disasters and cyber risks.

- **Testbed Selection**: We recommend selecting representative municipalities that face typical critical infrastructure challenges and common external threats, such as weather-related events. Cities like Houston and Norfolk, known for their vulnerability to disasters and their

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

critical infrastructure needs related to the Defense Industrial Base, would be ideal candidates for this initiative.

- **Public-Private Collaboration**: A successful observatory must prioritize public-private partnerships, bringing together government agencies, private sector stakeholders, and academic institutions. This collaboration will be essential for understanding diverse challenges and developing comprehensive solutions, ensuring that the observatory serves as a vital connector across sectors.
- **Focus on Grand Challenges**: The observatory should address grand challenges, such as leveraging AI and advanced technologies to enhance resilience. By focusing on these challenges in a real-world context, the observatory can generate insights and frameworks that effectively improve national cyber-physical resilience.
- **Community Engagement**: While there may be concerns from residents about participating in observatory municipalities, it's crucial to highlight the benefits of engagement. Living within these environments will facilitate practical learning and preparedness, ultimately enhancing community resilience.

By utilizing the observatory as a connector and testing ground for innovative solutions, we can ensure that research translates into meaningful advancements in infrastructure security and resilience across the country.

Advance Predictive Cyber Threat Intelligence Methodologies. To enhance the utility of cyber threat intelligence in building resilient systems, research should focus on developing predictive analysis methodologies that anticipate future threats rather than solely relying on retrospective analysis. This involves creating models that incorporate diverse data sources and leverage machine learning to forecast potential adversary actions. By advancing predictive capabilities, organizations can proactively address vulnerabilities and better allocate resources, ultimately improving system resilience and reducing risk.

Integrate Engineering Expertise into Cyber Threat Intelligence. To improve the accuracy and applicability of threat intelligence, research should prioritize the integration of engineering expertise into the intelligence production process. This involves developing frameworks that facilitate collaboration between cyber intelligence analysts and engineering subject matter experts, ensuring a comprehensive understanding of how critical infrastructure systems are designed and operated. By bridging this gap, threat intelligence can more effectively inform risk assessments and resilience strategies, leading to more robust protection of critical assets.

Investigate Defensive AI and ML Applications for Cyber Resilience. To counteract the adversarial use of AI and ML, research should explore defensive applications of these technologies to enhance cyber resilience. This includes developing AI-driven tools for automated vulnerability detection, defense design and optimization, threat prediction, and real-time response. By leveraging AI and ML defensively, organizations can stay ahead of adversaries, improving their ability to protect critical infrastructure from sophisticated cyber threats.

Direct Science and Technology Funding to Investigate "Break Glass" and Other Crisis Technologies. As demonstrated during the "Shields Up" U.S. government initiative ahead of the Russian invasion of Ukraine, there is value in increasing security postures in times of crisis. Unfortunately, maintaining a more robust security posture can strain operations, putting substantial burden on staff and systems. Similarly, recovery actions following a successful breach or attack can also strain operations, and past events have demonstrated that organizations

that respond quickly in the event of cyber attack can reduce overall damage.[3] Some past research has demonstrated the utility of these crisis technologies,[4] but additional R&D direction and focus would accelerate development and adoption. MITRE recommends that the research strategy allocate more R&D resources to enhance the resiliency of CPS against adversary attack.

[3] The 2015 cyber attack in Ukraine against three electricity distribution companies demonstrated the benefits associated with fast responses. In that case, the utility that quickly severed its virtual private network connections had the least interruptions in power and the fastest restoration times.

[4] One such example is Idaho National Laboratory's Constrained Communications Cyber Device, which can be used to restrict communications with protective relays in the event that an imminent attack on electric grid operations is suspected. (Additional information is available at https://inl.gov/national-security/prpc/.)