# PUBLIC SUBMISSION

**Received:** May 29, 2025
**Tracking No.** mba-2n9v-yjg5
**Comments Due:** May 28, 2025 **Submission Type:** Web

**Docket:** NSF-2025-OGC-0001
NITRD_FRDOC_0001

**Comment On:** NSF-2025-OGC-0001-0001
Request for Information: Development of a 2025 National Artificial Intelligence Research and Development Strategic Plan

**Document:** NSF-2025-OGC-0001-DRAFT-0307
Comment on FR Doc # 2025-07332

## Submitter Information

**Organization:** The CNA Corporation

## General Comment

See attached file(s)

## Attachments

The CNA Corp RFI Response 2025 AI Strat Plan

**Response to the Request for Information on the Development of a 2025 National Artificial Intelligence (AI) Research and Development (R&D) Strategic Plan**

**Responding organization**: **The CNA Corporation (CNA)**. CNA is an independent, non-for-profit research organization dedicated to the safety and security of the nation. For over 80 years, we have helped US leadership across the government address their most complex global, national security, and homeland security challenges. Our approach to research and analysis was built around the idea of placing scientists and analysts with operators who make day-to-day decisions. This operational perspective—understanding how and why decisions are made by our clients—drives everything we do. We work on emerging technology challenges with our military and intelligence clients through our Center for Naval Analyses; and civilian government organizations through our Institute for Public Research. We provide AI-related research, exercises, games and policy analysis across all domains. Based on the breadth of our client base we are pleased to offer the following recommendations for key research areas. **Please contact the following individuals with questions or for additional information:** Joseph Butcher, Vice President of Business Development; and Cherie Rosenblum, Vice President of Strategic Initiatives;

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 developing the 2025 National AI R&D Strategic Plan and associated documents without attribution.

**AI for Securing Critical Infrastructure.** The strategic importance of AI in safeguarding our nation's critical infrastructure cannot be overstated. Integrating AI into critical infrastructure is essential for resilience against current and emerging threats. For instance, natural disasters such as hurricanes, earthquakes, and floods pose significant risks to critical infrastructure. Research should focus on using AI for disaster preparedness and response, including predictive analytics, real-time monitoring, and automated response systems. AI can analyze vast amounts of data from various sources to predict the likelihood of natural disasters and their potential impact on infrastructure. This information can be used to develop proactive measures to mitigate the effects of disasters and ensure a swift and effective response.

Our research for clients in this area has shown that AI technologies can enhance the performance and efficiency of critical infrastructure systems by providing advanced capabilities for monitoring, control, and response, which is vital for maintaining the security and functionality of these systems. We see direct applications for AI in smart grid management, water resource management, and transportation network optimization.

Research should also focus on optimizing the human-machine interface for autonomous systems, ensuring appropriate human judgment in AI deployment. This involves designing systems that allow humans to effectively oversee and intervene in AI operations when necessary. Ensuring that AI systems can operate autonomously while

still enabling human oversight is crucial for maintaining control and accountability in critical infrastructure systems.

Research on AI integration should address factors that could introduce operational risks within critical infrastructure, including blind spots in current and near-future technology, inadequate operational considerations, and gaps in material development and testing, doctrine, training, and law and policy. Mitigating these risks requires a deliberate focus on comprehensively developing and testing capabilities, including robust concepts of operations, training, and doctrine development. Enhancing situational awareness and deconfliction capabilities can significantly reduce operational risks and improve the overall effectiveness of AI systems supporting critical infrastructure.

Additionally, research focused on processes for enhancing collaboration among federal partners is vital for effective AI integration. This can significantly improve AI integration within critical infrastructure by facilitating the sharing of information, resources, and expertise. Collaboration establishes broad stakeholder understanding of infrastructure dependencies and interdependencies within and across sectors and helps ensure that AI systems are developed and deployed in a manner that aligns with the needs and priorities of all involved parties. It also helps inform planning and preparedness to respond to emerging threats.

**Developing AI Use Cases.** As the use of AI systems expands across the private and public sectors, there is greater pressure to continually expand how, and when, AI technologies are used. Our research has shown that key to decision-making in this environment is to provide high-level government leadership with standard structures for evaluating the benefits of these technologies. This includes establishing a systematic approach to identify, assess, and prioritize AI applications that align with mission objectives and operational needs. This involves creating detailed evaluation criteria, methodologies, and tools that can be used consistently across different agencies and sectors to ensure that AI technologies are deployed effectively and efficiently. Each AI use case needs to be evaluated based on its potential for increased mission efficacy, operational constraints, data availability issues, implementation risks, and other factors. Research in this area should focus on:

*Creating Standardized Evaluation Frameworks*. This includes defining criteria for assessing the potential benefits, risks, and feasibility of AI applications, and providing guidelines for consistent and objective evaluation.

*Assessing Operational Constraints and Data Availability.* This includes studying the specific challenges faced by different agencies and sectors and developing solutions to overcome these barriers to AI adoption.

*Developing Risk Assessment Tools*. This includes developing methodologies for assessing technical, operational, and ethical risks, and providing actionable recommendations for mitigating risks.

*Enhancing Interagency Collaboration*. This includes developing standardized protocols for joint initiatives, collaborative decision-making, and coordinated AI deployment to ensure a unified approach to AI adoption.

*Evaluating Real-World Impact*. This includes developing tools and methodologies for studying the outcomes of AI deployments, identifying best practices, and providing recommendations for optimizing AI applications to maximize their value and effectiveness.

By focusing on these research priorities, the government can ensure that AI technologies are deployed in a manner that adds value and meets the real-world needs of government agencies.

**AI Policy, Guidance, and Risk Reduction**. Developing policies that foster innovation while safeguarding public trust and upholding the highest standards of accountability is essential for effective AI implementation. Establishing comprehensive frameworks, guidelines, and protocols that provide clear direction on AI governance, data management, and security protocols. These structures ensure that AI deployment is consistent, transparent, and aligned with national priorities. At CNA, we understand that putting in place structure and oversight are an integral part of delivering capabilities that create value for our clients. Research in this area should focus on:

*Developing Comprehensive AI Governance Frameworks.* These frameworks should outline roles, responsibilities, and processes for AI oversight. This includes defining standards for AI use and security protocols to ensure responsible AI deployment.

*Interagency Coordination and Collaboration.* This includes developing methods for enhancing coordination and collaboration among federal agencies through standardized protocols for information sharing, joint initiatives, and collaborative decision-making processes to ensure a unified approach to AI governance.

*Risk Assessment and Mitigation Strategies*. Research should focus on creating robust risk assessment frameworks that consider operational, technical, and ethical risks, and provide actionable recommendations for mitigating these risks.

*AI Policy Development and Implementation*. Research should support the development of comprehensive AI policies that address key issues such as data management, algorithmic transparency, and accountability. This includes studying best practices from other sectors and countries to inform policy development and ensure effective implementation.

By focusing on these research priorities, the government can establish a solid foundation for AI governance that promotes innovation while ensuring ethical and responsible AI deployment. CNA stands ready to support these efforts.

**AI for Enhancing Cybersecurity.** One of the most significant emerging threats to critical infrastructure is cyber-attacks, including those driven by AI. These attacks can target various systems, including power grids, water supply networks, transportation systems, and communication networks. AI-driven cybersecurity defense mechanisms are central to protecting national security and maintaining the integrity of our digital infrastructure. Research should focus on developing AI solutions that can detect and mitigate cyber threats, including anomaly detection, pattern recognition, and real-time response capabilities to counteract AI-driven cyber threats. Further, enhancing AI threat intelligence capabilities to identify and analyze adversarial AI activities is essential. Using AI to process and interpret vast datasets provides actionable insights for decision-makers.

Our research has consistently shown that AI can significantly enhance cybersecurity measures. For example, our work on developing risk assessment frameworks and conducting red-teaming and safety tests has demonstrated the effectiveness of AI in identifying and mitigating cyber vulnerabilities. This research is crucial for ensuring that AI systems are robust and capable of withstanding adversarial attacks. Additionally, our exploration of the operational, logistical, and strategic implications of AI for cybersecurity through various gaming and exercises has provided valuable insights into how AI can be leveraged to enhance national security.

**Developing Effective Counter AI Capabilities.** Developing counter AI capabilities is essential to mitigate the risks posed by adversarial AI technologies and ensure that our military and intelligence operations remain secure and effective. It is vital to prioritize the characterization of adversary efforts regarding AI and how they plan to use that technology for a military edge over the US. Our research has shown that understanding the AI capabilities and intentions of adversaries informs and supports the development of effective countermeasures. For example, our work with the US Space Force (USSF) involved evaluating how AI applications could be developed and applied across the service, creating frameworks for prioritization at both mission and service levels. This research is essential for ensuring that the US can maintain its strategic advantage and protect national security interests. Research in this area should focus on:

*Characterization of Adversary AI Efforts***.** Prioritizing the understanding of how adversaries are developing and employing AI technologies for military purposes is fundamental. This research will help identify potential threats and inform the development of countermeasures to mitigate these threats.

*AI-Driven Threat Detection and Mitigation.* Developing AI solutions that can detect and mitigate adversarial AI threats is essential. This includes anomaly detection, pattern recognition, and real-time response capabilities to counteract AI-driven cyber and physical threats.

*Development of Robust Defense Mechanisms.* Creating robust AI defense mechanisms that can withstand and counteract adversarial AI attacks is vital. This involves exploring

AI-driven cybersecurity solutions and developing standards for secure AI system design.

*Strategic Foresight and Adaptation.* Conducting strategic foresight to understand the implications of emerging AI technologies and adapting military strategies accordingly is necessary to maintain a competitive edge. CNA's strategic foresight efforts have helped government agencies understand the risks, opportunities, and actions of emerging AI technologies. This research is vital for maintaining a strategic advantage in AI and ensuring that the US is prepared to counter adversarial AI threats.

*Adversarial AI Testing and Evaluation.* CNA has developed methodologies for adversarial AI testing and evaluation, providing a framework for assessing the robustness of AI systems against potential adversarial attacks. Our research includes exploring the use of AI for electronic warfare and the development of countermeasures to protect AI systems from jamming and spoofing.

**Conclusion.** By emphasizing these research areas, the government can harness the full potential of AI to safeguard critical infrastructure, enhance cybersecurity, and counter adversarial AI threats. CNA stands ready to support research and development in these and other AI priority areas. As a nonprofit organization with no commercial ties to AI providers, we offer objective data-driven analysis to help the government navigate the complexities of AI and ensure a secure and resilient future for the nation.

Submitted by:
The CNA Corporation
3003 Washington Blvd.
Arlington, VA

Joseph Butcher, Vice President of Business Development;
Cherie Rosenblum, Vice President of Strategic Initiatives;