From Exploration to Execution – Why Half Measures Fail

How to Operationalize AI Across Government Enterprises

Government agencies have the potential to revolutionize their enterprise operations through AI-powered transformation. However, they also face implementation risks that demand careful consideration. Successfully operationalizing AI within an enterprise requires agencies to balance both immediate opportunities and long-term transformation while maintaining robust safeguards against potential dangers.

SHADOKA®
LEAD. INNOVATE. TRANSFORM.

CACI
EVER VIGILANT

RESEARCH & EDITORIAL TEAM

Faisal Hoque
Founder, SHADOKA, NextChapter, and other companies. A #1 *Wall Street Journal* bestselling author. His newest book, *TRANSCEND: Unlocking Humanity in the Age of AI*, was named a "must read" by the Next Big Idea Club and debuted as a *USA Today*, *Los Angeles Times*, and *Publishers Weekly* bestseller. Contributor at MIT's IDEAS Social Innovation program and the Swiss business school IMD.

Prof. Thomas H. Davenport
President's Distinguished Professor of Information Technology and Management, Babson College, and Fellow, MIT Initiative on the Digital Economy. Author of *All In on AI*, *Working with AI*, and *Only Humans Need Apply*.

Erik Nelson
Senior Vice President, CACI International Inc. Enterprise IT Market Leader responsible for driving strategic vision and account growth within the $2B Enterprise IT market for CACI. Passionate to develop leaders and motivate them to perform at their highest potential.

Albert Lulushi
Chief Technology Officer, Enterprise IT, CACI International Inc. Leads teams of senior technologists working in partnership with Business Development, Capture, Proposal, and Operations to architect, design, and develop cost estimates, and implement cross-domain solutions in support of the company's strategic goals.

Dr. Paul Scade
Partner, SHADOKA, and author and researcher specializing in philosophy, management theory, and psychology. Paul has researched and taught at the University of Pittsburgh, Central European University, and the University of Exeter. He is currently an Honorary Fellow at the University of Liverpool.

Dr. Pranay Sanklecha
Partner, SHADOKA, and author and researcher specializing in technology and philosophy. Formerly a professor of philosophy at the University of Graz, Pranay has lectured at universities around the world, including Princeton, Vienna, Seattle, and Minnesota.

Executive Summary

Government agencies have the potential to revolutionize their enterprise operations through AI-powered transformation. However, they also face potential implementation risks that demand careful consideration. The successful implementation of AI within an enterprise requires agencies to balance immediate opportunities with long-term transformation while maintaining robust safeguards against potential dangers.

This paper presents a comprehensive approach to AI implementation for government agencies. It begins by examining the current state of AI in government and business. The paper showcases successful deployments across administrative, military, and intelligence functions, as well as key relevant private sector applications. The paper then explores the organizational impacts of AI adoption, emphasizing that effective implementation requires fundamental changes to organizational structures, workflows, and human capital management – including the emergence of new competencies such as Digital Workforce Management.

Government agencies must move beyond piecemeal or fragmented approaches to AI implementation, as these half measures inevitably lead to missed opportunities and potential risks. Success requires a comprehensive transformation strategy that balances immediate tactical implementations with long-term strategic vision, supported by structured frameworks that address both innovation and risk management.

To help agencies navigate this complex landscape, we present two complementary frameworks: the OPEN framework (Outline, Partner, Experiment, Navigate) for harnessing the potential of AI and the CARE framework (Catastrophize, Assess, Regulate, Exit) for managing associated risks. These frameworks provide structured approaches for both seizing opportunities and mitigating dangers while ensuring alignment with agency missions. The paper concludes by identifying three AI architectural approaches and three key focus areas in which agencies can achieve near-term value through AI implementation. Analytical AI, generative AI, and agentic AI have immense potential over a short-term horizon of 1-2 years. Information Technology Service Management, Information Technology Operations, and Government Security represent "low-hanging fruit" that agencies can pursue today while building the capabilities and cultures needed for more ambitious AI transformations in the future.

01

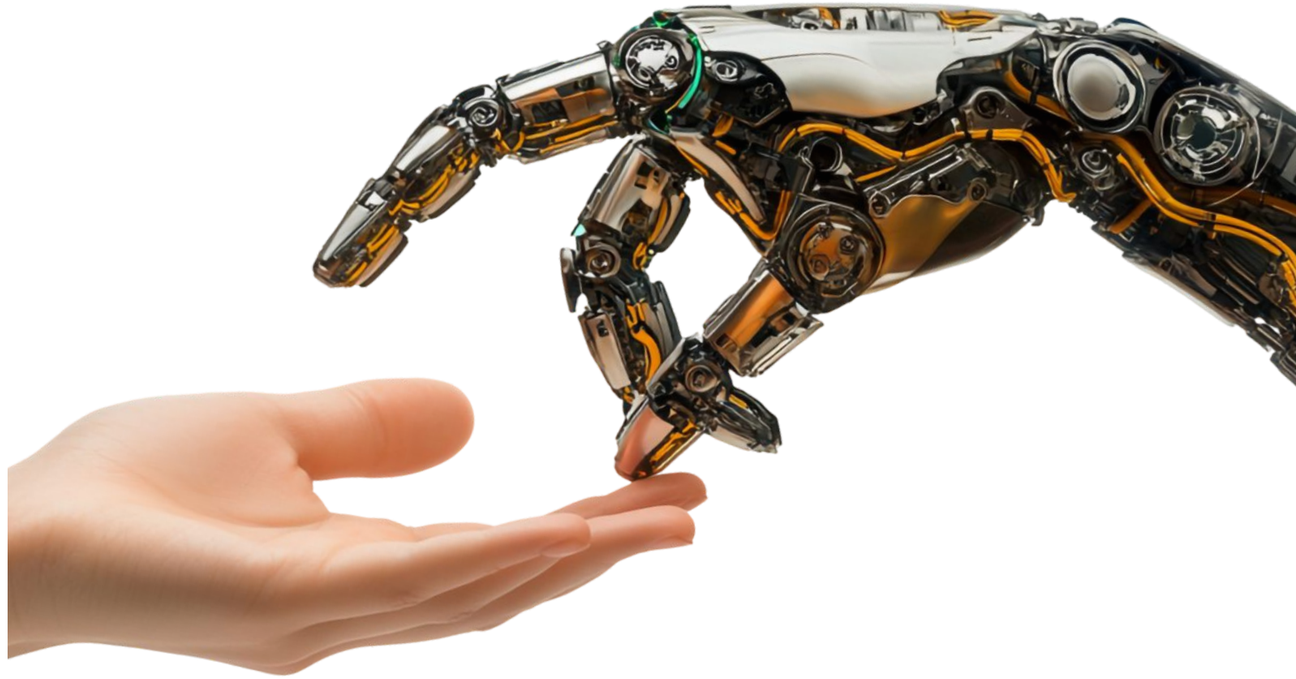
AI Opportunities & Challenges

Artificial Intelligence (AI) will fundamentally reshape how U.S. government agencies operate, make decisions, and serve citizens and the national interest. This technology has unprecedented potential to enhance operational efficiency, improve decision-making capabilities, and revolutionize service delivery. Yet this same revolutionary power brings with it profound risks that demand careful consideration. Government agencies must navigate a complex landscape in which the promise of AI-driven transformation must be balanced against the need to maintain robust safeguards and ensure responsible implementation.

The successful deployment of AI within government agencies requires more than just technical expertise or strategic vision – it demands a fundamental reconceptualization of how organizations operate in an age of intelligent systems. This paper presents a comprehensive framework for government agencies seeking to harness the potential of AI while managing its inherent risks. Drawing on future-oriented research and current real-world implementations across administrative, military, and intelligence functions, we outline both the immediate opportunities that AI presents for government agencies and the longer-term transformational possibilities that lie ahead. Central to our analysis is the recognition that achieving success with AI requires agencies to move beyond traditional change management approaches and adopt new systems of thinking specifically designed for operating under conditions of rapid change and unprecedented complexity.

The Potential of AI

The deployment of AI-powered solutions by government agencies has already demonstrated remarkable potential across the full spectrum of government operations, from streamlining administrative processes to enhancing military capabilities. These early implementations reveal both the transformative power of AI and the unique challenges that agencies face in deploying this technology. While private sector organizations can often focus solely on efficiency and profitability, government agencies must balance multiple competing priorities, including operational effectiveness, citizen service, security requirements, and public accountability. Despite these complex demands, the success of existing AI implementations demonstrates that agencies can harness this technology effectively to achieve their missions while maintaining necessary safeguards and controls.



Government Administrative Use Cases

- The Centers for Disease Control uses natural language processing to read medical records and automatically code causes of death. MedCoder automates nearly 90% of records, a significant improvement over the less than 75% achieved by the previous system.[1]
- FEMA's Incident Management Workforce Deployment Model uses machine learning methods to analyze large historical datasets to support personnel deployment planning in response to disasters.[2]
- The VA uses an AI model to read incoming mail and then automatically route it to the relevant employee, cutting processing times by 90%.[3]

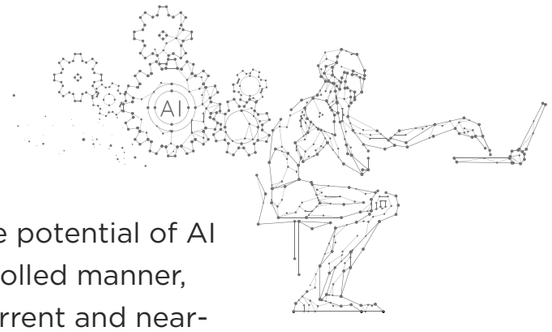
Government Military and Intelligence Use Cases

- The Pentagon's Joint All-Domain Command & Control (JADC2) program integrates multi-service data with machine learning and predictive analytics to reduce battlefield decision cycles and improve the quality of decisions.[4]
- DISA's Thunderdome Zero Trust Project uses AI to improve threat detection accuracy and speed by analyzing patterns across multiple security domains.[5]
- The Defense Innovation Unit uses AI to help protect the Alaska fisheries by implementing AI algorithms that can detect vessels by analyzing information collected via synthetic aperture radar.[6]

Private Sector Use Cases Relevant to Government

- Internal Knowledge Management. Morgan Stanley's AI @ Morgan Stanley Assistant makes information from more than 100,000 internal documents accessible to the company's financial advisors.[7] The AI @ Morgan Stanley Debrief system summarizes client conversations with their permission.[8]
- Customer Service. The e-commerce credit company Klarna's customer service AI agent now handles two thirds of all customer service chats, achieving high satisfaction ratings while carrying the workload of 700 customer service agents.[9]
- Healthcare Access. Amazon's One Medical uses AI-powered intelligent task routing to connect patients quickly and accurately to the most appropriate sources of care.[10] The “Good Doctor” smartphone app created by Ping An in China performs initial triage, preliminary diagnosis, and provides a preliminary treatment plan before the patient has a virtual or in-person consultation, and arranges delivery of medications to the patient's home.[11]
- IT Service Management. ServiceNow is using AI capabilities across a broad range of IT Service Management (ITSM) functionalities to increase efficiency and improve client outcomes, including generative AI for routine task automation, predictive analytics for incident management, and agentic AI for performing tasks and fixing problems.[12]

AI Today & Tomorrow



Taking advantage of the transformative potential of AI today, and doing so in a safe and controlled manner, starts with gaining clarity about the current and near-future capabilities of this technology. The two categories of AI capabilities that currently offer the greatest potential for government agencies are:

Analytical AI. These systems focus on data analysis, pattern recognition, and predictive modeling. Current analytical AI models leverage the increasingly sophisticated processing and reasoning capabilities of machine learning algorithms to deliver results with a speed and accuracy that cannot be matched by any other digital tool. Successful deployments of analytical AI by government agencies include FEMA's disaster response analytics, which uses machine learning models based on geospatial data and sensor data to provide "situational awareness" for disaster response.[13]

Workflow Automation / Deterministic AI is a sub-category of Analytical AI. AI systems in this category are used to automate routine information-based processes and administrative tasks, including making simple decisions. The technology that powers workflow automation combines analytical AI with deterministic AI. While analytical AI components generate information about a situation, the deterministic AI model then ensures a consistent rule-based response. Workflow automation is widely used in the federal government, including robotic process automation (RPA) implementations in benefits processing at the VA[14] and ServiceNow deployments for IT service management across federal agencies.[15]

Generative AI. Generative AI uses complex machine learning models to create new content, from text and code to images and decision scenarios. While current media discussion of AI focuses on the promise of generative AI models, both business and governmental use cases remain in the experimental phase. However, there are many current areas of pilot activity in the U.S. government, including defense and intelligence use cases. For instance, the Department of Defense is using generative AI for mission planning and simulations, the CIA for pattern recognition and translation, the Department of Homeland Security for threat detection and emergency planning, and the FBI for criminal investigations.[16] While these agencies must carefully manage challenges related to data security and AI bias, generative AI remains vital for modernizing national security operations.

These two classes of AI technology define the current landscape for AI use cases in government. Looking to the immediate future, the next frontier of AI implementation in government agencies will be the deployment of agentic AI.

Agentic AI. AI agents are AI systems that will pursue defined objectives with increasing levels of autonomy, marking a fundamental shift from today's tools-based approach to an era in which AI agents become active participants in government operations. In January 2024, in a harbinger of the age of agentic AI, OpenAI released Operator, an AI agent that can go to the web and perform tasks such as making restaurant bookings, scheduling flights, and buying groceries.[17] The evolution of these kinds of capabilities promise to transform governmental processes by providing autonomous decision-making and implementation capabilities that can adapt dynamically to changing circumstances. Agentic AI will offer proactive threat identification and response functionality and the possibility of complex coordination among multiple agents and AI systems across departments.

AI RISK AND REWARD

Reward	Risk		
Faster data analysis *Improved budgeting* *Better predictions* *Enhanced human decisions*	*Algorithmic bias* *Privacy concerns* *Lack of transparency* *Factual errors*	**Analytical AI** including	*FEMA disaster response* *Pentagon JADC2 program* *DISA's Thunderdome Zero Trust*
Efficient processing *Lower costs* *Improved consistency* *Always on*	*Limited flexibility* *Systemic errors* *Technical vulnerability*	**Workflow Automation / Deterministic AI**	*US Army's Project Convergence* *CDC cause of death coding* *VA mail processing*
Clearer documents *Content creation* *Scenarios and simulations* *Enhanced communication*	*Hallucinations* *Copyright issues* *Reputational harm* *Security threats*	**Generative AI**	*DoD mission planning* *DHS Cyber Threat Detection* *US Army acquisition activities*
		Near Future	
Autonomous action *Problem solving* *Dynamic decision-making* *Rapid adaptation*	*Ethical boundaries* *Lack of accountability* *Failure cascades* *Public fear*	**Agentic AI**	*AI Scientists* *OpenAI Operator* *ServiceNow Orchestrator*

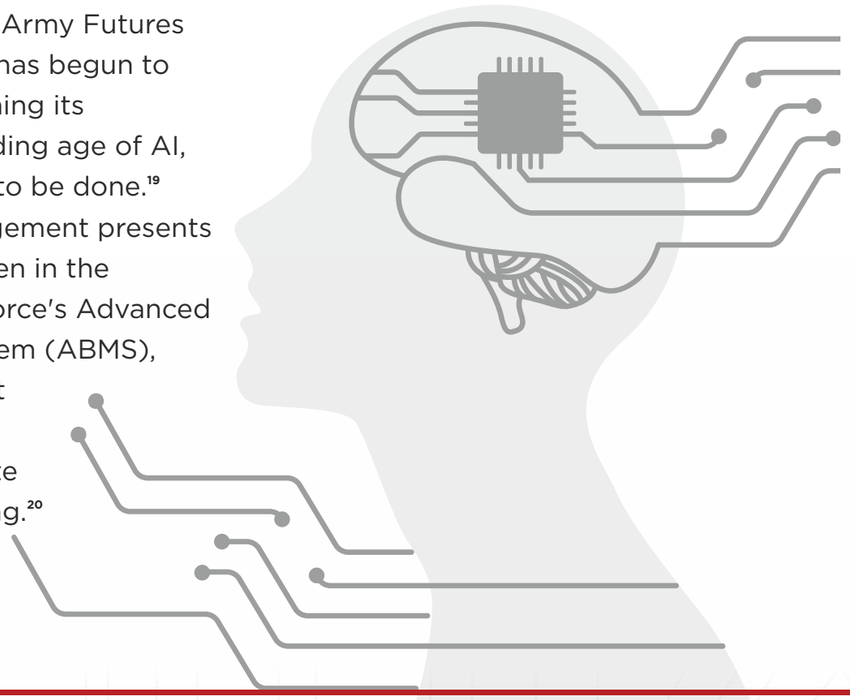
Figure 1. Risk, Rewards, and Examples of Different Types of AI

The Challenge of Implementing AI Successfully

Organizations typically find it easy to experiment with AI and explore its capabilities, but much harder to successfully deploy this technology. A recent study by BCG revealed that while 98% of companies are actively exploring AI, only 26% have developed operational products and a mere 4% have achieved significant returns on their investments.[18] These figures reflect the range of organizational, technical, and regulatory obstacles that hinder the effective implementation of AI systems.

Key challenges to overcome include:

Cultural Resistance. A notable barrier to the successful implementation of AI is cultural resistance to change, and in particular resistance to digital transformation. The challenge inherent in changing cultures is exacerbated by extensive skill gaps that reinforce resistance. The Army Futures Command, for example, has begun to invest extensively in training its personnel for the impending age of AI, but much more remains to be done.[19] Moreover, change management presents significant hurdles, as seen in the deployment of the Air Force's Advanced Battle Management System (ABMS), which struggled to adapt established operational procedures to incorporate AI-driven decision-making.[20]



Technical Integration. Integrating AI into legacy systems has proven especially difficult for government agencies, with the Department of Defense and intelligence agencies encountering major challenges in modernizing decades-old infrastructure.[21] For instance, the Joint All-Domain Command and Control (JADC2) initiative faced significant obstacles in connecting disparate and incompatible data systems across service branches.[22] Data quality and standardization adds a further layer of complexity. The Defense Innovation Unit has reported difficulties in harmonizing data from diverse sources, including commercial, classified, and partner-nation inputs.[23] The need to ensure efficient implementation without compromising security represents a special challenge for government agencies, and especially those responsible for national security. The Defense Information Systems Agency's (DISA) Thunderdome project, for example, has grappled with the challenge of balancing zero-trust security principles with the need to maintain full interoperability.[24]

Regulatory and Oversight Issues. Establishing clear accountability frameworks for AI decisions has been a persistent challenge for government agencies.[25] For example, the Chief Digital and Artificial Intelligence Office of the Department of Defense has had to design new frameworks, toolkits, and strategic and implementation pathways to ensure AI systems adhere to ethical standards without compromising operational effectiveness.[26] Creating transparent audit mechanisms has also proven difficult, as agencies seek to maintain security classifications while enabling traceability in AI decision-making.

These interconnected challenges highlight the multifaceted complexities involved in implementing AI at scale. Comprehensive strategies are needed that address organizational, technical, and governance dimensions and integrate these into planning from the start of a project, rather than attempting to solve problems as they arise.

The Chief Innovation and Transformation Officer: Leadership Tailored for the Challenges of AI[27]

The complexity and uncertainty inherent in AI implementation demands a new kind of organizational leadership. Most organizations treat AI implementation as a primarily technical challenge – and current technology leadership roles reflect this mindset. Yet, in a recent survey, 91% of large company data leaders said "cultural challenges/change management" are the primary obstacle keeping their organizations from becoming data-driven, while only 9% said technology challenges were the key barrier.[28] According to another survey, 85% of IT leaders say that CIOs are increasingly becoming changemakers in their organizations, but only 28% call leading transformation their top priority..[29]

While traditional CIOs and CTOs focus primarily on project execution and operational management, the Chief Innovation and Transformation Officer (CITO) takes a holistic view across the entire organization, steering innovation that touches all aspects of identity and culture. By establishing an Office of Innovation and Transformation led by a CITO, organizations create the capacity to manage both the technical and human dimensions of AI deployment. The CITO role extends beyond technical implementation to oversee the strategic, cultural, and ethical aspects of AI transformation as well, including the management of AI personas and the development of new organizational capabilities. This broader mandate enables organizations to navigate the challenges of cultural resistance, technical integration, and regulatory oversight while maintaining alignment between AI initiatives and organizational purpose.

AI Readiness for Government Agencies

Preparing agencies for AI adoption is now an imperative. A series of executive orders from the president, along with supporting memoranda from the office of budget management, charge Federal agencies with "using safe and secure artificial intelligence (AI) in innovative ways to improve government efficiency and mission effectiveness." In pursuit of this goal, "agencies must procure effective and trustworthy AI capabilities in a timely and cost-effective manner," mirroring existing IT accountability structures rather than creating new layers of approvals.[30]

The successful implementation of AI demands more than just technical integration – it requires fundamental organizational transformation. Piecemeal adoption of AI solutions, while tempting for its apparent simplicity, will inevitably lead to fragmented systems and missed opportunities. Instead, organizations must embrace a holistic approach that recognizes AI's transformative impact across all operational dimensions. This approach revolves around three critical themes: cultural and structural evolution, reimagining work, and managing the digital workforce.

Cultural and Structural Evolution. Government agencies will need to undertake profound cultural and structural change to fully realize the potential of AI. Traditional hierarchical structures and siloed departments will have to give way to more fluid, adaptive modes of organization that are capable of rapid response to AI-driven insights. This requires creating new organizational structures that facilitate human-AI collaboration, updating decision-making processes to balance AI-generated insights with the maintenance of human oversight, and reforming training programs to emphasize digital literacy, critical thinking, and AI interaction skills. Additionally, performance metrics must evolve to measure the effectiveness of human-AI collaboration rather than solely human output.

Reimagining Work. The relationship between human workers and AI is reshaping the fundamental nature of work. This transformation goes far beyond simple task automation or workforce reduction, amounting to a fundamental shift in how work is conceptualized and executed. Traditional employee roles will pivot toward functions that rely on uniquely human capabilities, such as strategic thinking, emotional intelligence, and complex decision-making. A 2023 report by IBM found that 40% of global workers will need to reskill within three years due to AI integration.[31] New positions focused on AI oversight, training, and optimization will emerge, and hybrid teams combining human and AI skills will become the standard rather than the exception.

Managing the Digital Workforce. A key aspect of this transformation is the emergence of the "digital workforce" – AI agents and personas that work alongside human employees. This changing workforce mix adds an additional layer of complexity to organizational transformation. Technology departments will need to transition from maintaining systems to managing an evolving portfolio of AI capabilities. AI personas will take on specialized roles such as data analysis or customer service, while human managers will oversee blended teams of human and AI workers. Organizations will need to create new frameworks to evaluate and optimize human-AI collaboration.

Successfully managing the new digital workforce will demand specialized skills, including an understanding of the capabilities and limitations of both humans and AI, the ability to foster effective collaboration between the two, and a commitment to ethical AI deployment. Managers will also need to negotiate the psychological and social dynamics of human-AI interaction to ensure a productive and harmonious working environment.

02
Structured Systems of Thinking for Implementing AI

Systematic Thinking

The implementation of government technology initiatives has historically been challenging. According to a World Bank Report, between 80-90% of public sector technology projects are full or partial failures, and fewer than 20% can be deemed successes.[32] At first glance, the prospect of successfully implementing AI capabilities appears even more daunting, because AI introduces additional layers of uncertainty and complexity that traditional management approaches simply cannot handle. For instance, in January 2025, the United Kingdom's Department of Work and Pensions (DWP) announced that it had canceled at least half-a-dozen promising AI pilots, citing "frustrations and false starts." In particular the DWP highlighted difficulties in ensuring that the systems in question are "scalable, reliable [and] thoroughly tested."[33]

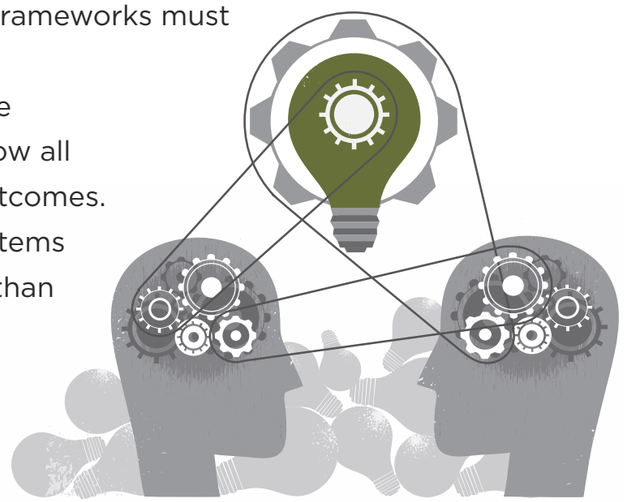
The uncertainty relating to AI is of a qualitatively different type to that involved in other technology projects, because even the parameters of change remain unknown. It is not just that we do not know what will happen, but that we do not even know what variables will matter or how the technology will evolve in the future. For example, it is currently unclear how AI might transform basic concepts like work, decision-making, or human relationships. We do not know whether entirely new capabilities will emerge and, if they do, what that will mean for humanity. And we do not yet know whether AI will develop consciousness or emotions.

This type of uncertainty makes traditional planning approaches, which rely on being able to identify relevant variables, inadequate for dealing with long-term AI planning. Government agencies that create fixed implementation plans based on current AI capabilities risk not just failure but actively harmful outcomes as the technology rapidly evolves in directions at odds with initial assumptions.

In addition, partial or piecemeal approaches to AI implementation can create blind spots. When dealing with interdependent systems the boundaries of which we cannot fully map, incomplete or failed solutions can spread through critical government operations. A narrow focus on technical integration while ignoring cultural transformation, or an emphasis on efficiency metrics that overlooks ethical implications, is almost certain to undermine the ability of agencies to carry out their missions.

These features of AI mean that the traditional model of "plan then execute" that has guided government technology initiatives for decades cannot be relied upon. When both the capabilities of the technology and its effects on organizational systems are evolving in unpredictable ways, static implementation plans become obsolete before they can be completed.

Government agencies need a new approach built around systems of thinking that are specifically designed to navigate continuous change and adaptation. These systems must fulfill two critical requirements. First, they must provide comprehensive guidance for managing change across entire organizations, since partial solutions will inevitably fail when dealing with interdependent systems that we cannot fully map. Second, these frameworks must be engineered for resilience and adaptability, built to help navigate situations in which we cannot know all the variables or predict all the outcomes. We need to engineer resilient systems that thrive on uncertainty rather than trying to eliminate it.



OPEN and CARE

These challenges can be addressed by deploying systematic approaches to AI implementation. Publicly available frameworks that address important elements of the AI journey include the National Institute for Standards and Technology AI Risk Management Framework[34] and the use case identification and prioritization framework developed by researchers at Harvard's Kennedy School of Governance.[35] In this paper we outline a comprehensive framework for implementing AI developed by CACI's strategic partner Faisal Hoque (see *Transcend: Unlocking Humanity in the Age of AI*, Post Hill Press, 2025). The approach involves using two integrated frameworks, each designed to handle a different dimension of AI implementation. The OPEN framework (Outline, Partner, Experiment, Navigate) creates a structured pathway for realizing the transformative potential of AI while the CARE framework (Catastrophize, Assess, Regulate, Exit) establishes systematic safeguards against the technology's inherent risks.

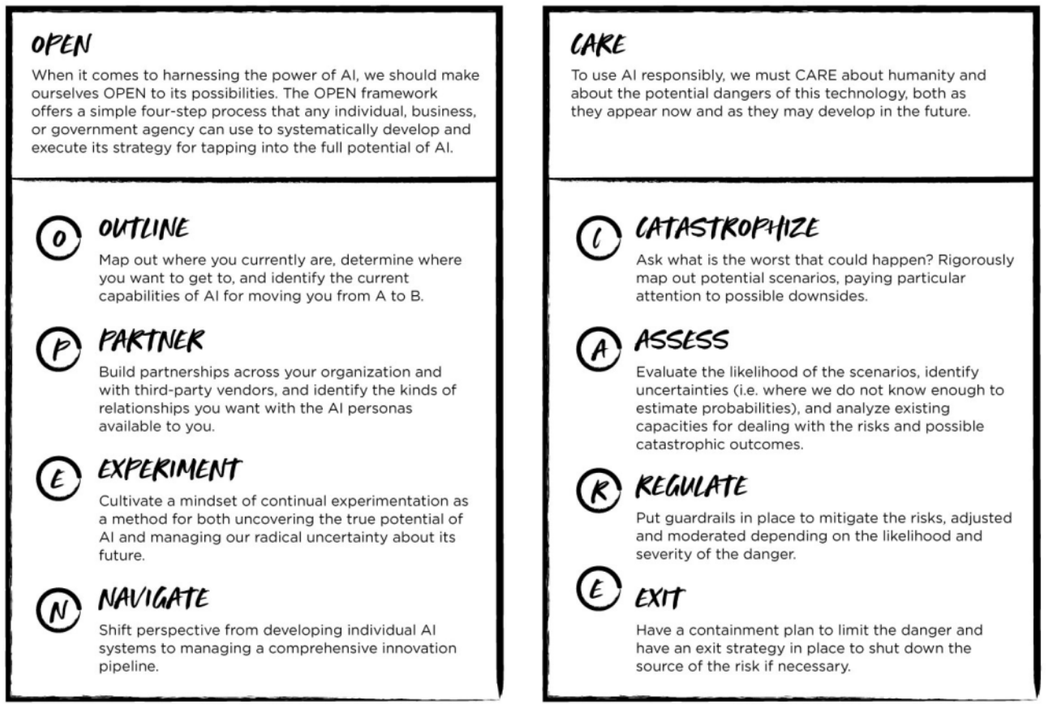
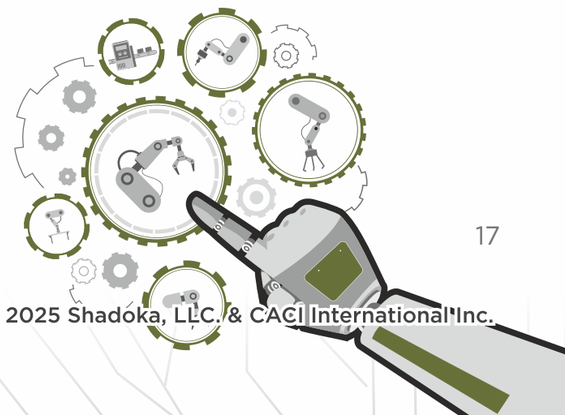


Figure 2. The OPEN and CARE Frameworks. Adapted from F. Hoque (2025) *Transcend: Unlocking Humanity in the Age of AI*, Post Hill Press. (copyright Faisal Hoque)

The OPEN methodology leads organizations through four essential phases of AI implementation. In the Outline phase, agencies explore their needs and identify specific AI opportunities that align with their mission. The Partner phase focuses on building the necessary capabilities, both through internal collaboration and in partnership with carefully selected external vendors. During the Experiment phase, agencies test AI solutions in controlled environments in which failure can be contained and learned from. Finally, the Navigate phase guides the expansion of successful pilots into full-scale implementation and provides a high-level and immediately accessible portfolio-style view of the organization's AI innovation pipeline.

Working in parallel with OPEN, the CARE framework ensures that agencies maintain robust defenses against AI-related risks. The framework begins with the Catastrophize step – a systematic effort to identify potential modes of failure and worst-case outcome scenarios for AI systems. This is followed by the Assess phase, in which agencies analyze the likelihood and potential impact of identified risks. The Regulate phase establishes controls and monitoring systems to manage these risks, while Exit planning ensures agencies can rapidly shut down or pivot away from AI systems that prove problematic.

These complementary frameworks address both sides of the AI challenge, embedding and enabling two essential mindsets for AI implementation: optimism about the potential of this powerful new technology balanced with deep caution about its risks. While OPEN empowers agencies to pursue AI's transformative potential, CARE puts in place the guardrails that make bold action possible. This dual approach allows organizations to move forward confidently with AI initiatives while maintaining appropriate safeguards against potential negative outcomes



This balanced approach finds practical expression through the integration of innovation and risk management processes using a Portfolio and Financial Management (PfM) approach.

The innovation management process, guided by the OPEN framework, allows agencies to maintain a comprehensive view of AI opportunities across different time horizons. Near-term opportunities like IT service management can be viewed and prioritized in relation to medium-term possibilities in areas like generative AI and the longer-term transformative potential of agentic AI. By managing these opportunities as a coherent portfolio rather than as isolated initiatives, agencies can optimize their allocation of resources and ensure that immediate implementations build toward longer-term capabilities.

At the same time, the CARE framework enables agencies to apply PfM principles to risk management. Just as financial portfolios balance different types of investments to optimize returns while managing risk, agencies can develop portfolios of AI initiatives that systematically balance opportunities and risks. Some projects may be relatively low-risk implementations of proven technology, while others might involve cutting-edge applications that demand more robust controls. The portfolio approach embedded in the frameworks allows agencies to identify and manage those risks holistically.

Adopting this kind of structured and strategically minded approach will deliver significant improvements when compared to the fragmented approaches often seen in government technology rollouts. Leaders who embrace and excel at this balanced method will be uniquely equipped to tackle the unparalleled challenges and seize the transformative opportunities that come with AI.

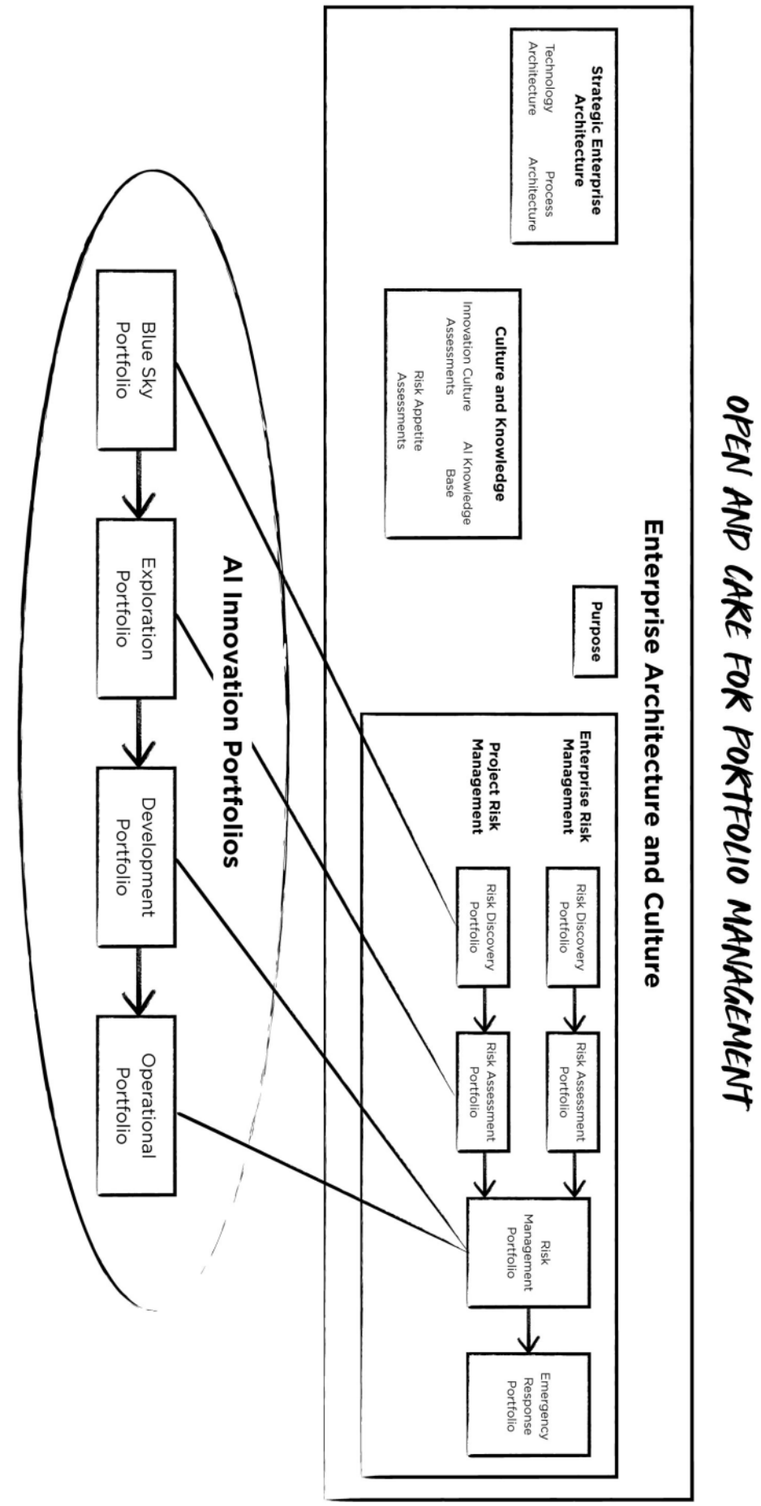
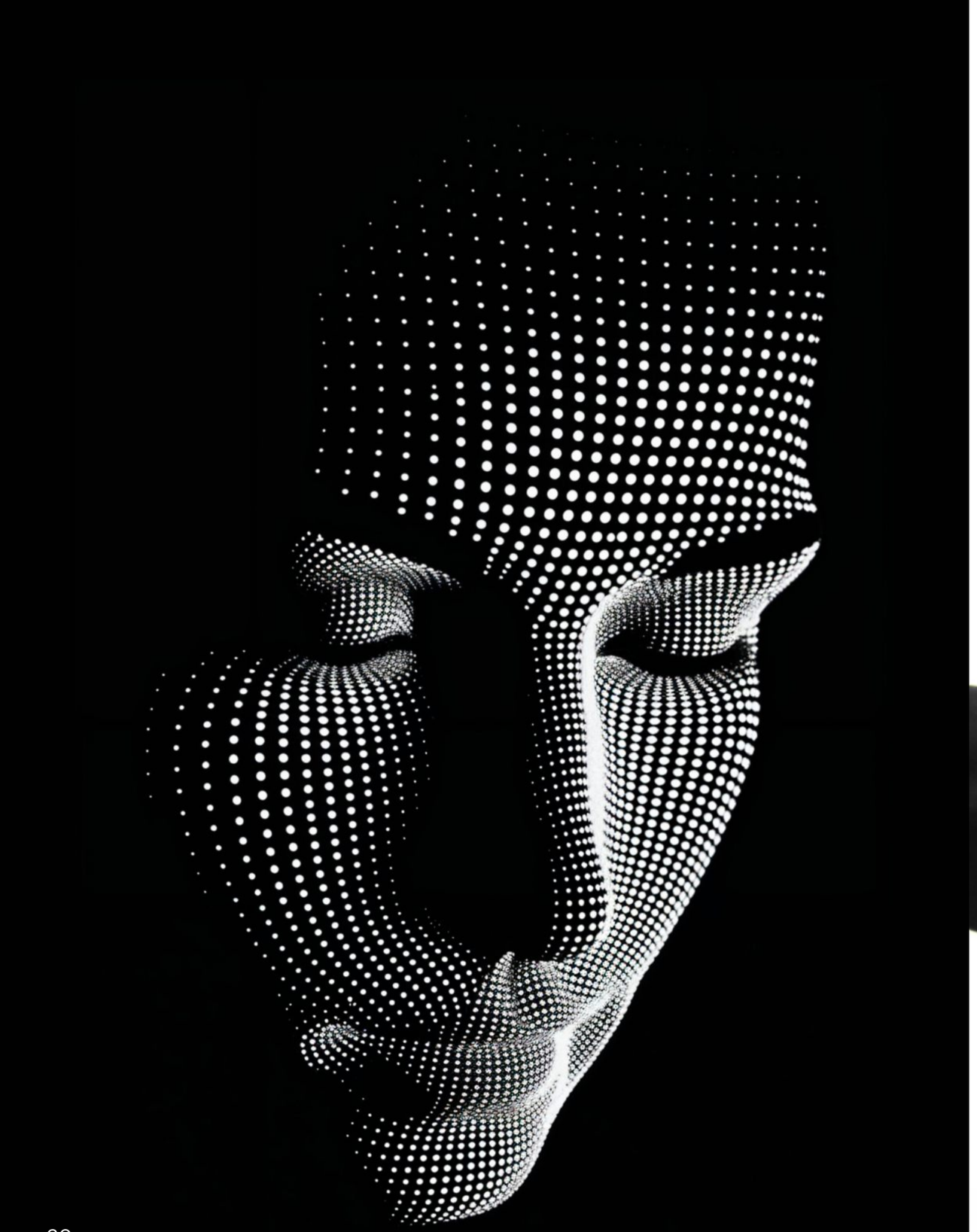
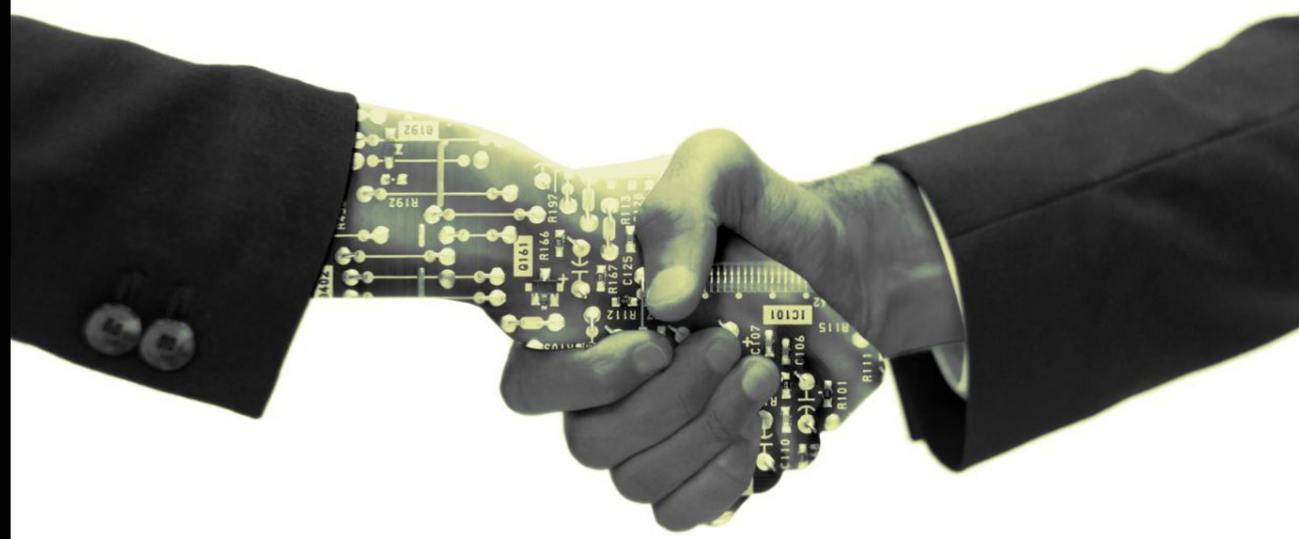


Figure 3. Integrating OPEN and CARE (copyright Shadoka, LLC.)



03

Near-Term Opportunities for Government Agencies



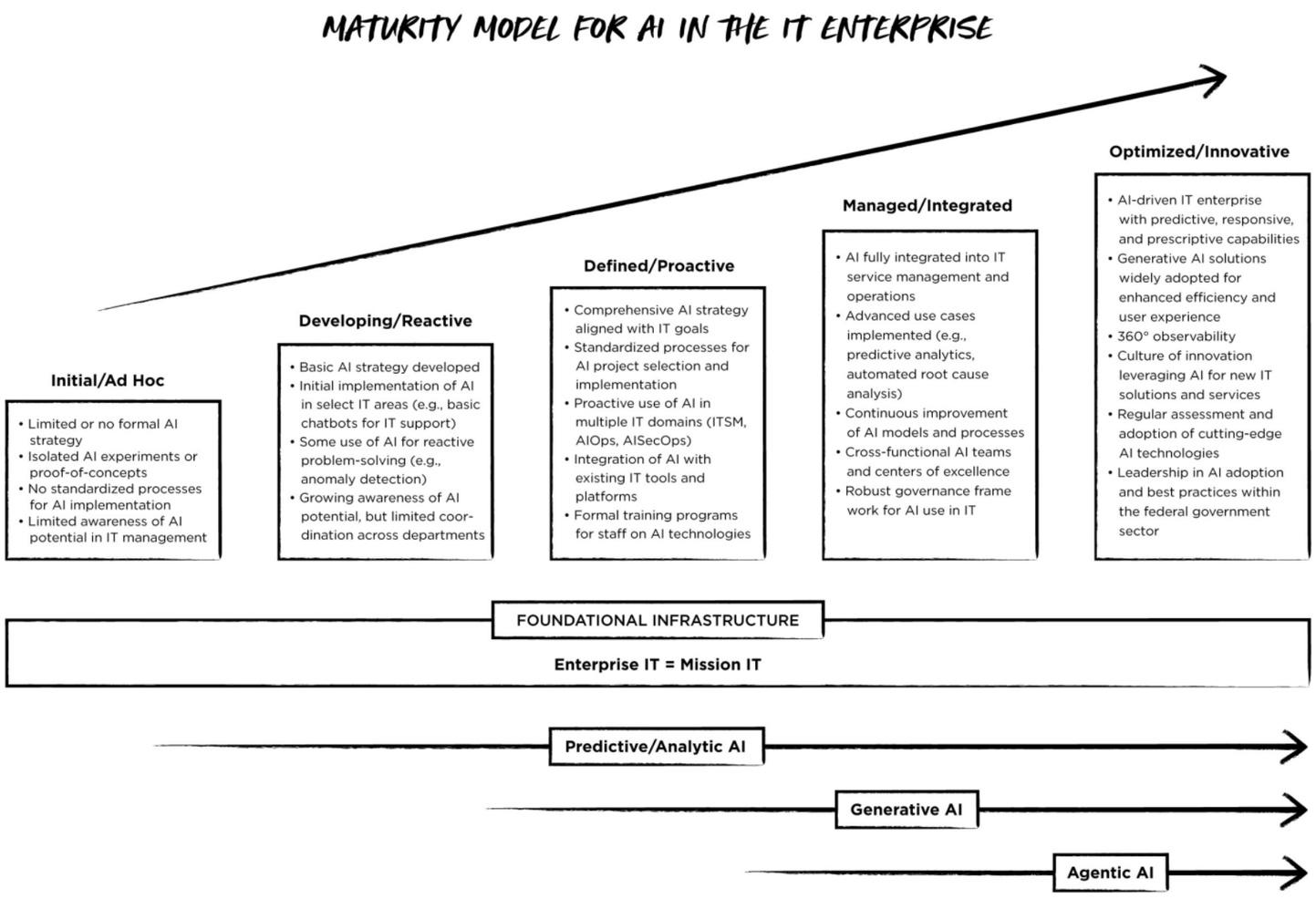


Figure 4. The AI Maturity Model (copyright CACI International Inc.)

While the long-term potential of AI for transforming government operations is vast, agencies do not need to wait for future technological breakthroughs to begin realizing significant value. Several mature AI capabilities are ready for deployment today, offering immediate opportunities to improve efficiency and effectiveness across government operations. Others will move from the pilot stage to operational viability over the next two years. Systematically implementing these capabilities offers government agencies the chance to seize this low-hanging fruit, achieving meaningful short-term results using proven AI solutions and existing technical frameworks. These projects can serve both as valuable initiatives in their own right and as steppingstones toward more ambitious AI transformations, allowing agencies to build institutional experience and capabilities while delivering tangible benefits to citizens. To maximize the value of these early implementations while building toward more advanced capabilities, the President and his advisors have mandated that agencies must now think systematically about their AI maturity journey.[35] Part of this maturity journey involves developing capabilities and institutional knowledge across three key architectural approaches. Predictive/analytic AI (including deterministic AI and workflow automation models) are the bedrock of all stages of AI maturity. As organizations advance, they will add competencies around generative AI that go beyond developing and managing simple support service chatbots. In the most mature stages of their AI journey, organizations will integrate the emerging capabilities of agentic AI, deploying autonomous decision-making capabilities alongside human agents. Each architecture requires its own tools and perspectives. Success depends on first understanding these distinct approaches and then unifying them into a coherent implementation strategy.

At the Initial/Ad Hoc stage, organizations operate in a largely chaotic environment with isolated pockets of AI experimentation. These agencies may run individual AI projects but they lack a systematic approach to implementation. There is little to no formal AI strategy at this stage, and experiments or proofs-of-concept remain disconnected from broader organizational goals.

As agencies move to the Developing/Reactive stage, they begin to show repeatable capabilities. A basic AI strategy emerges, and initial implementations appear in select areas – typically involving simple applications like chatbots for IT support. While these implementations demonstrate potential, they remain largely reactive, addressing immediate needs rather than strategic objectives.

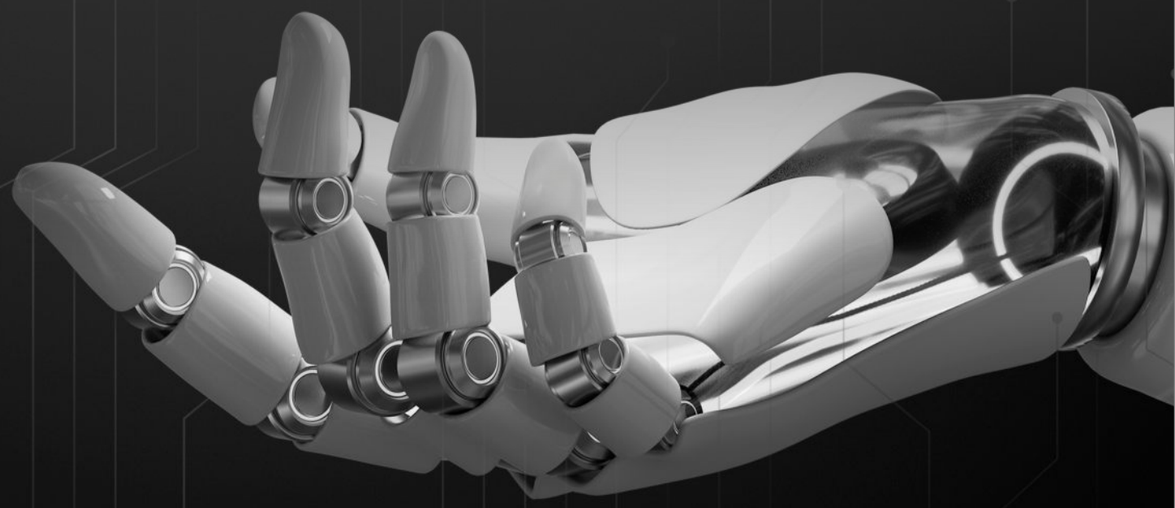
At the Defined/Proactive level, agencies achieve what maturity models call "threshold capabilities." They develop comprehensive AI strategies aligned with IT goals and they implement standardized processes for AI project selection and implementation. Integration between key process areas begins, although response times to new opportunities remain slow and inconsistent.

Agencies that reach the Managed/Integrated stage demonstrate disciplined, consistent management characterized by quantitative performance measurements. AI becomes fully integrated into IT service management (ITSM) and operations, with advanced use cases implemented across multiple domains. Cross-functional AI teams emerge, and robust governance frameworks guide implementation.

Finally, at the Optimized/Innovative stage, agencies achieve full agility and adaptability. They develop predictive and prescriptive AI capabilities, widely adopt generative AI solutions, and maintain a culture of continuous innovation. These organizations influence and shape how other government agencies and departments use AI rather than simply following established practices.

It is important for agencies to assess where they stand in their AI maturity journey because organizations cannot leap directly from initial experiments to fully optimized AI operations. This reality drives two key principles for AI implementation.

- First, agencies must select projects appropriate to their current maturity level. An organization at the Initial/Ad Hoc stage attempting to implement fully integrated autonomous AI operations is extremely likely to fail, wasting resources and potentially undermining support for future AI initiatives.
- Second, agencies should choose implementations that serve dual purposes: delivering immediate operational value while laying the foundations for higher levels of AI maturity. For example, implementing basic workflow automation not only creates near-term efficiency gains but also helps organizations develop the process discipline needed for more sophisticated AI applications.



AI Architectural Approaches

Analytical/Predictive AI
Analytical AI using traditional machine learning excels at prediction. Government agencies have broad needs for predictive capabilities, including domains such as economic and budget forecasting, understanding changing weather patterns, predictive maintenance for equipment and machinery, predictive and precision medicine, and even prediction of software licenses that are likely to expire.

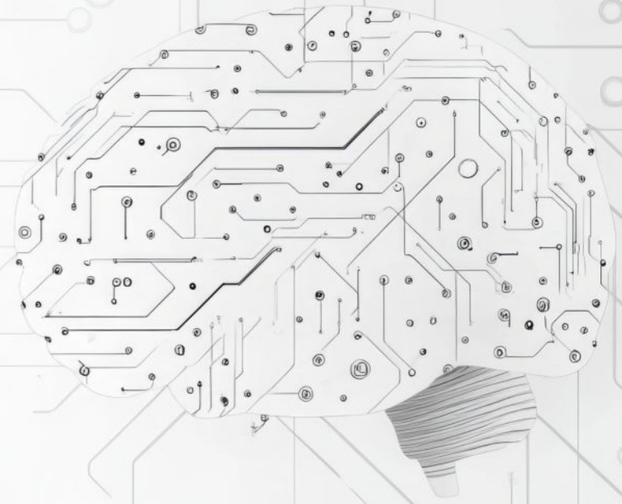
Analytical AI models can increasingly be generated automatically (AutoML), which opens up predictive modeling to people who are not professional data scientists. Another trend in the private sector is to set up "AI factories," which use AI platform software in order to reuse data and variables across an organization and speed up modeling activities. Analytical AI for IT management can forecast potential issues hours or days before they impact services. This enables IT teams to shift from reactive firefighting to proactive problem prevention.

Generative AI
The McKinsey Global Institute estimates that generative AI will add between $2.6 and $4.4 trillion in annual value to the global economy and will automate half of all work activities between 2040 and 2060. U.S. security and intelligence operations should position themselves at the forefront of this transformation.

Several areas offer immediate opportunities for value creation. In signals intelligence, generative AI can rapidly process and translate intercepted communications across multiple languages, identifying patterns and connections that human analysts might miss. This technology is particularly valuable when dealing with non-standard language use, dialects, and coded communications. Scenario planning represents another high-value opportunity. Generative AI can create detailed simulations of potential security threats, helping agencies prepare for a wider range of contingencies than traditional planning methods allow. These AI systems can generate thousands of scenario variations, systematically exploring how different variables might interact in a crisis. Intelligence report generation and analysis offers a third promising domain. AI can draft preliminary intelligence reports by synthesizing information from multiple sources, allowing human analysts to focus on validation and deeper analysis rather than initial collection and compilation. The technology is particularly effective at identifying discrepancies between sources and flagging areas that require human attention.

Agentic AI
Agentic AI represents the next major evolution in artificial intelligence capabilities, marking a shift from AI as a sophisticated tool to AI as an autonomous partner in government operations. While still in early stages, agentic AI is already demonstrating significant potential in pilot programs across government agencies. Early implementations show that AI agents can independently manage complex tasks like monitoring cybersecurity threats, coordinating emergency response activities, and orchestrating supply chain logistics – adapting their actions in real-time based on changing conditions and new information.

The true power of agentic AI lies in its ability to operate as part of larger systems of coordinated agents. For example, in disaster response scenarios, multiple AI agents could work together to monitor weather conditions, analyze population movements, coordinate emergency services, and manage resource distribution – all while continuously communicating with each other and human operators. This multi-agent approach enables a level of operational coordination and rapid response that would be impossible with traditional command and control structures. As the technology matures, agentic AI is expected to transform how government agencies handle complex, multi-dimensional challenges that require real-time coordination across multiple domains and stakeholders.



High-Potential Focus Areas

AI in Government IT Service Management

Information Technology Service Management represents one of the most promising areas for immediate AI implementation. The private sector has already embraced AI within ITSM functions, with 88% of companies leveraging AI capabilities in this domain.[37] Government agencies are positioned to achieve similar benefits, but they also face unique challenges in implementation. As the experiences of the Social Security Administration and NASA demonstrate, legacy systems, stringent security requirements, and workforce concerns create important hurdles that must be overcome.[38,39]

Here's how organizations can leverage AI effectively in ITSM today:

- **Immediate Response Improvements:** Generative AI can automatically analyze incoming service tickets, understand their content, and route them to the appropriate support teams instantly. This intelligent routing eliminates manual triage time and significantly reduces overall resolution times. For example, a networking issue would be immediately directed to the network team rather than passing through multiple hands first.

- **24/7 Automated Support:** Generative AI-powered chatbots serve as a first line of defense, handling common user issues around the clock. These systems can guide users through basic troubleshooting steps, reset passwords, or provide immediate answers to frequently asked questions. This automation allows human IT staff to concentrate on solving more complex technical challenges that require their expertise.

- **Proactive Issue Prevention:** By analyzing historical data patterns in system performance and user requests, analytical AI models can identify potential problems before they impact users. For instance, AI might detect increasing memory usage patterns that could lead to system failures and then alert IT teams to take preventive action.

- **Enhanced Knowledge Management:** Generative AI can transform how organizations capture and utilize their IT knowledge. The system continuously learns from every interaction, automatically updating and organizing the knowledge base. It can:

  - Extract solutions from successful ticket resolutions
  - Identify gaps in documentation
  - Suggest updates to existing articles
  - Link related issues and solutions
  - Make relevant information easily discoverable

- **Advanced Analysis Capabilities:** Numerous use cases include:

  - Natural language processing enables AI to understand user requests in plain language, ensuring accurate interpretation of problems and faster access to solutions.
  - Smart classification automatically fills in critical ticket information, reducing manual data entry and ensuring consistent categorization.
  - Pattern recognition connects current issues with similar past incidents and their solutions, accelerating problem resolution.
  - Incident trend analysis identifies emerging major issues by recognizing patterns across multiple tickets, enabling proactive responses to systemic problems.
  - Predictive analytics estimates resolution times based on historical data, helping teams better manage resources and set accurate expectations.

These capabilities work together to create a more efficient, responsive, and intelligent IT service management system that continuously improves over time while reducing the workload on IT staff.

29

AI in Government Information Technology Operations

The adoption of AI in information technology operations (AIOps) is accelerating rapidly across sectors. According to Gartner, 70% of companies will have implemented some degree of structured automation in their IT operations by 2025, up from just 20% in 2021.[40] A 2023 MIT survey of 600 data and technology leaders found that 89% of companies had already adopted AI in at least some IT functionality, with 67% reporting broad-based adoption. By 2025, AI is expected to play a critical role in IT operations at 49% of organizations.[41]

Despite the challenges posed by legacy systems and cybersecurity requirements, AI and machine learning are transforming IT operations by enabling systems to monitor, analyze, and respond to infrastructure issues at a scale impossible for human teams. At its core, AIOps brings unprecedented visibility and automation to enterprise IT environments through real-time monitoring and predictive capabilities. In practice, AIOps platforms continuously analyze massive amounts of data across an organization's entire IT infrastructure. They automatically detect performance anomalies, correlate seemingly unrelated events to identify root causes, and often resolve issues before users are impacted. For example, an AIOps system might notice subtle changes in application response times, correlate this with increasing memory usage and historical patterns, and automatically allocate additional resources before performance degrades.

The key capabilities of AIOps that add immediate value to Government agencies include:

- **Intelligent Anomaly Detection:** Advanced analytical AI algorithms identify unusual patterns in real-time, spotting potential issues across networks, servers, and applications that human operators might miss. This extends beyond simple threshold monitoring to understanding complex patterns of normal behavior and flagging true anomalies.

- **Event Correlation and Analysis:** When issues occur, AIOps cuts through the noise of thousands of alerts to identify related events and their root causes. Rather than treating each alert separately, the system connects the dots between multiple warnings to reveal underlying problems. For instance, it might link seemingly separate alerts about network latency, database slowdowns, and application errors to identify a failing network switch as the root cause.

- **Dynamic Resource Optimization:** AIOps continuously monitors resource usage across the IT environment and automatically adjusts allocations to optimize performance and cost. During peak periods, it can automatically scale up resources to maintain service levels, then scale them back during quiet periods to control costs.

OPEN and CARE for Government Information Technology Operations

The OPEN framework provides a structured approach to implementing these capabilities. In the outline phase, agencies should focus on mapping their current capabilities and identifying gaps where human teams struggle to maintain comprehensive coverage. The partner phase is crucial here, guiding agencies as they seek vendors with proven experience in government IT operations and a deep understanding of federal security requirements. Experimentation should begin with passive monitoring systems that run parallel to existing operations, allowing agencies to validate AI insights before acting on them. Once these are validated, the focus can then shift to gradually expanding both the scope of monitoring and the degree of automated response.

The CARE framework is particularly important in the technology operations field given the critical nature of government systems. Agencies must carefully map potential failure cascades, asking how an AI decision in one system might impact connected operations. Assessment should focus heavily on security implications, particularly around access controls and data handling, while the Regulation phase will establish clear thresholds for autonomous AI action versus human review. Perhaps most importantly, agencies must maintain robust manual fallback capabilities that can be activated instantly if AI systems need to be disengaged.

Implementation can begin today with a systematic audit of current monitoring capabilities and pain points. This audit should pay particular attention to areas in which human teams are overwhelmed by data volume or are struggling to maintain 24/7 coverage. With this information in hand, agencies can begin evaluating AI-powered monitoring solutions that align with their security requirements and technical architecture.

AI in Government Information Security

AI is fundamentally transforming information security by providing intelligent, automated defense capabilities that can operate at machine speed while simultaneously creating new vulnerabilities that must be managed. For instance, as bad actors weaponize AI, and cyber threats become more sophisticated and frequent, traditional manual security monitoring and response methods can no longer effectively protect organizations.[42] The Department of Homeland Security has integrated AI into its threat detection and border security operations, while the National Security Agency employs AI systems for real-time cyber threat detection.[43] While these implementations must contend with both AI-powered threats and potential system vulnerabilities, the technology remains crucial for maintaining effective modern security operations in the face of persistent and increasing threats from adversaries.

AI technologies enable security teams to detect, analyze, and respond to threats in real-time, while continuously learning and adapting to new attack patterns. Modern AI-powered security platforms can process vast amounts of security data across networks, endpoints, and cloud environments to identify potential threats. For example, these systems can use analytical AI to detect subtle patterns of malicious behavior that might indicate an advanced persistent threat (APT), automatically block suspicious activities, and provide security teams with detailed analysis for further investigation.

The core security capabilities enabled by AI include:

- **Advanced Threat Detection:** AI algorithms continuously monitor network traffic, system logs, and user activities to identify potential security threats. Unlike traditional rule-based systems, AI can detect novel attack patterns and zero-day threats by recognizing subtle deviations from normal behavior. For instance, it might detect data exfiltration attempts that are deliberately designed to evade traditional security controls.
- **Behavioral Analytics:** AI systems build detailed profiles of normal user and system behavior, enabling them to quickly identify suspicious activities. This might include unusual login patterns, unexpected data access, or anomalous network connections that could indicate compromised credentials or insider threats.
- **Automated Incident Response:** When threats are detected, AI can automatically initiate response actions to contain and mitigate the threat before significant damage occurs. This ranges from blocking suspicious IP addresses to quarantining affected systems or triggering additional authentication requirements.
- **Predictive Security:** By analyzing historical attack patterns and current threat intelligence, AI systems can predict potential security incidents and recommend preventive measures. This enables organizations to proactively strengthen their security posture against emerging threats.
- **Continuous Compliance Monitoring:** AI automates the monitoring and reporting of security controls, ensuring continuous compliance with regulatory requirements while reducing manual audit effort. The system can instantly flag compliance violations and provide detailed audit trails of security events.

This integration of AI into security operations creates a more resilient and adaptive defense system that can protect against sophisticated cyber threats while reducing the burden on security teams. It enables organizations to maintain robust security at scale, even as the threat landscape continues to evolve.

ROADMAP AND MILESTONES FOR AI IN THE IT ENTERPRISE

	Initial/Ad Hoc	Developing/Reactive	Defined/Proactive	Managed/Integrated	Optimized/Innovative
AI in IT Service Management (AITSM)	• Basic chatbot for simple IT support queries • AI pilot for ticket classification • Assess current ITSM processes for potential AI integration points	• AI-powered chatbot with NLP • Automated ticket classification across all IT support categories • AI-assisted knowledge article recommendations	• AI-driven similarity matching • AI clustering to identify emerging issues • Establish governance frame-work for AI use in ITSM processes	• Predictive analytics for proactive problem management • AI-powered virtual agents • AI capabilities across all major ITSM processes	• Continuous learning AI models that improve ITSM • Advanced NLP for context-aware IT support • AI-driven service level prediction
AI in IT Operations (AIOps)	• Implement basic anomaly detection for key IT systems • AI pilot for log analysis in a limited scope • Assess current operations processes for potential AI integration points	• AI-powered event correlation • Automated root cause analysis for common IT issues • AI-assisted performance monitoring for critical applications	• AI-driven predictive analytics for capacity planning • ML models for automated incident triage and routing • Centralized data lake for AIOps	• End-to-end AIOps platform integrating monitoring, analytics, and automation • AI-powered self-healing capabilities • AI-powered closed-loop remediation processes	• Cognitive automation for complex IT workflows and decision-making • Advanced AI models for real-time performance optimization • AI-driven, dynamic resource allocation
AI in Cybersecurity Operations (AISecOps)	• Basic AI-powered anomaly detection for network traffic • AI pilot for log analysis in Security Information and Event Management • Assess current security operations processes for AI integration points	• AI-assisted threat detection and alerting system • Automated user behavior analytics (UBA) • AI-powered phishing detection	• AI-driven Security Information and Event Management • ML models for automated threat hunting and investigation • AI-assisted compliance monitoring and reporting	• AI-powered Security Orchestration and Automated Response platform • Advanced AI models for real-time threat intelligence analysis • AI-driven vulnerability and threat scoring and prioritization	• Cognitive AI for autonomous decision-making • Advanced AI models for predictive threat modeling • Adaptive policies and controls
Generative AI	• Basic chatbot for FAQs in IT support • GenAI pilot for simple knowledge article creation • Assess potential use cases for generative AI across IT processes	• AI-powered user chat summarization • Automated generation of basic incident resolution notes • Creating simple how-to guides based on existing documentation	• AI-driven knowledge SOPs discovery system • Automated creation of knowledge articles • Governance framework for generative AI use in content creation and KM	• Advanced conversational AI for complex IT support • GenAI for automated root cause analysis reports • GenAI capabilities across multiple IT platforms (e.g., ITSM, PPM)	• Cognitive AI for content generation across all domains • Advanced generative models for complex technical documentation • AI-driven adaptive learning systems
360° Observability and Single-Pane-of-Glass (SPoG)	• Basic monitoring dashboards • SPoG pilot to integrate data from 2-3 critical into a single view • Assess current observability gaps	• Centralized log aggregation and analysis • Initial version of a SPoG dashboard • Basic infrastructure and app performance correlation	• Comprehensive data ingestion • Advanced analytics for cross-domain correlation • Standardized observability practices and metrics	• AI-driven anomaly detection and alerting • Deploy fully integrated SPoG platform • Automated, context-aware incident handling	• Predictive analytics for proactive issue resolution • Cognitive AI autonomous decision-making, self-healing • Dynamic, real-time service modeling

Figure 5. Roadmap and Milestones (copyright CACI International Inc.).

Conclusion

Government agencies stand at a defining moment. The AI revolution represents the greatest opportunity for transforming government operations in a generation. The potential benefits are immense: enhanced service delivery, improved decision-making, and unprecedented operational efficiency. But to deliver on this opportunity, agencies will need to be equipped with the right tools to navigate the challenges ahead.

What makes this moment particularly significant is the transformative potential of AI across all government operations. By adopting thoughtful implementation strategies, agencies can integrate AI capabilities in ways that align with and enhance their core missions. This integration requires evolved approaches to management that embrace both innovation and responsible governance – approaches that recognize AI as a strategic asset rather than simply another technology deployment.

The key to navigating this landscape successfully lies in adopting structured systems of thinking that are specifically designed for implementing transformative technologies. Agencies that embrace frameworks like OPEN and CARE will be better positioned to seize immediate opportunities while building toward long-term transformation. They will be able to move forward confidently with AI initiatives while developing the organizational capabilities and cultures needed to adapt and evolve as AI systems continue to change.

The six domains explored in Part 3 of this paper – the broad areas of analytical AI, generative AI, and agentic AI, and the specific areas of IT Service Management, IT Operations, and Government Information Security – offer immediate opportunities for agencies that wish to build their AI capabilities today and develop those capabilities over the next two years. By starting with these low-hanging fruit while simultaneously developing their capacity for managing more comprehensive AI implementations, agencies can build the organizational muscles needed for more ambitious transformations.

As AI becomes increasingly integral to all aspects of government operations, those agencies that master a balanced approach – pursuing AI's potential while thoughtfully managing implementation – will be ideally positioned to deliver enhanced value to citizens in our AI-enabled future. With proper planning, structured frameworks, and clear maturity pathways, government agencies can confidently embrace AI's transformative potential as a cornerstone of modern public service.

Contact

Erik Nelson,
Senior Vice President, Enterprise IT, CACI International Inc.
eknelson@caci.com

Albert Lulushi,
Chief Technology Officer, Enterprise IT, CACI International Inc.
albert.lulushi@caci.com

Faisal Hoque,
Founder, Managing Partner, Shadoka, LLC.
faisal.hoque@shadoka.com

Endnotes

1 https://www.cdc.gov/surveillance/data-modernization/technologies/ai-ml.html?
2 Federal Emergency Management Agency – AI Use Cases | Homeland Security
3 https://news.va.gov/press-room/va-decreases-mail-processing-time-for-claims-intake/?
4 https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/
5 https://www.dau.edu/sites/default/files/2024-11/DAU%20Sero%20Trust%20%20Thunderdome%20%2020241119_0.pdf?
6 https://www.akbizmag.com/industry/fisheries/illegal-fishing-ai/
7 https://www.businessinsider.com/morgan-stanley-ai-chatgpt-used-nearly-all-wealth-management-teams-2024-4
8 https://www.morganstanley.com/press-releases/ai-at-morgan-stanley-debrief-launch?
9 https://www.klarna.com/international/press/klarna-ai-assistant-handles-two-thirds-of-customer-service-chats-in-its-first-month/?
10 https://www.aboutamazon.com/news/innovation-at-amazon/amazon-one-medical-launches-ai-tools-for-better-patient-care?
11 https://www.forbes.com/sites/tomdavenport/2021/03/02/the-future-of-work-now-good-doctor-technology-for-intelligent-telemedicine-in-southeast-asia/?
12 https://www.servicenow.com/company/media/press-room/gartner-mq-ai-apps-itsm.html?
13 https://govciomedia.com/how-geospatial-imaging-and-it-inform-femas-disaster-response/
14 https://www.socom.mil/care-coalition/SiteAssets/Conference-2024/20240401%20Final%20Automation%20Presentation.pdf?
15 https://www.twd.com/what-we-do/cloud-services/servicenow/?
16 https://www.defense.gov/News/Releases/Release/Article/3489803/dod-announces-establishment-of-generative-ai-task-force/ ; https://fedscoop.com/how-the-cia-is-using-generative-ai-lakshmi-raman/ ; https://www.fbi.gov/investigate/counterintelligence/emerging-and-advanced-technology/artificial-intelligence
17 https://openai.com/index/introducing-operator/
18 “Where’s the Value in AI”, Boston Consulting Group Report, October 2024. https://web-assets.bcg.com/a5/37/be4ddf26420e95aa7107a35aae8d/bcg-wheres-the-value-in-ai.pdf
19 https://www.nationaldefensemagazine.org/articles/2020/6/10/army-futures-command-boosting-ai-training?
20 https://www.airandspaceforces.com/air-forces-new-abms-czar-talks-integration-challenges-initial-assessments/?
21 https://www.airandspaceforces.com/air-forces-new-abms-czar-talks-integration-challenges-initial-assessments/?
22 National Academies of Sciences, Engineering, and Medicine. Advanced Battle Management System: needs, progress, challenges, and opportunities facing the department of the air force. 2022.

23 https://defensescoop.com/2024/09/04/diu-data-mesh-solution-unify-distribution-across-dod-networks/
24 https://www.afcea.org/signal-media/cyber-edge/disa-may-move-beyond-thunderdome-prototype
25 https://www.gao.gov/assets/gao-21-519sp.pdf
26 https://www.ai.mil/Initiatives/Responsible-AI/
27 http://sloanreview.mit.edu/article/why-ai-demands-a-new-breed-of-leaders/
28 https://static1.squarespace.com/static/62adf3ca029a6808a6c5be30/t/67642c0d40b42a7d7e684f49/1734618125933/2025+AI+%26+Data+Leadership+Executive+Benchmark+Survey+120624.pdf
29 https://www.cio.com/article/2088578/state-of-the-cio-2024-change-makers-in-the-business-spotlight.html
30 https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government ; https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf ; https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf https://www.whitehouse.gov/wp-content/uploads/2025/02/AI-Memo-Fact-Sheet.pdf
31 https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/augmented-workforce
32 https://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-pub-replacement-public.pdf
33 https://www.theguardian.com/technology/2025/jan/27/ai-prototypes-uk-welfare-system-dropped
34 https://www.nist.gov/itl/ai-risk-management-framework
35 https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/working.papers/MRCBG%20Working%20Paper%202024-02_AI%20for%20the%20People.pdf
36 https://www.whitehouse.gov/wp-content/uploads/2025/02/AI-Memo-Fact-Sheet.pdf
37 https://www.atlassian.com/whitepapers/state-of-ai
38 Office of the Inspector General, Social Security Administration. Audit Report: Legacy Systems Modernization and Movement to Cloud Services, 2024.
39 https://arstechnica.com/space/2024/09/eminent-officials-say-nasa-facilities-some-of-the-worst-theyve-ever-seen/
40 https://www.gartner.com/en/articles/4-predictions-for-i-o-leaders-on-the-path-to-digital-infrastructure
41 https://www.databricks.com/sites/default/files/2023-07/ebook_mit-cio-generative-ai-report.pdf
42 According to the Government Accountability Office’s 2024 report, federal agencies reported 32,211 security incidents in FY2023, an increase of 9.9% from the previous year. https://www.whitehouse.gov/wp-content/uploads/2024/06/FY23-FISMA-Report.pdf
43 https://www.meritalk.com/articles/new-nsa-ai-tool-to-automate-cyber-threat-detection/

SHADOKA®

LEAD. INNOVATE. TRANSFORM.

SHADOKA.COM

CACI

EVER VIGILANT

CACI.COM