PUBLIC SECTOR SERVICES

Unlocking AI Model Innovation

Transforming Federal R&D Through Next-Generation AI Infrastructure

A FEDERAL AGENCY ROAD MAP FOR NEXT-GENERATION AI INFRASTRUCTURE

Executive Summary: Federal agencies must act decisively to maintain America's AI leadership. This paper provides agency leaders with a practical framework for establishing AI programs that balance innovation with security, speed with compliance, and transformation with risk management. The recommendations herein are based on current federal mandates, emerging best practices, and lessons learned from early agency implementations.

1. STRATEGIC CONTEXT

Federal Agencies Face an AI Imperative

Your agency operates at a critical inflection point. The rapid advancement of artificial intelligence presents both unprecedented opportunities and complex challenges for federal operations.[1] While private sector adoption accelerates, government agencies must navigate unique requirements: statutory obligations, security imperatives, and public accountability standards that commercial entities do not face.[2]

Current federal policy establishes clear expectations: Agencies must integrate AI capabilities while maintaining robust governance frameworks.[3] The challenge is not whether to adopt AI, but how to do so responsibly and effectively within existing operational constraints.

What Agency Leaders Need to Know About AI Models

For decision-making purposes, agency leadership should understand AI models as sophisticated analytical tools that process data to support mission objectives. Unlike traditional software that follows predetermined rules, AI models learn patterns from data to generate insights, predictions, or recommendations.[4]

Defining AI Models in the Federal Context

An AI model, as defined by 15 U.S.C. § 9401(3), is "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."[5] This definition distinguishes AI from basic automation, standard calculations, or simple "if-then" rule-based systems. AI models introduce learning capabilities that enable pattern recognition, adaptation, and improved performance over time through exposure to data.

The Fundamental Shift in Computing Paradigm

Traditional computing systems operate on explicit instructions—if X, then Y. Every outcome is predetermined by programmers. AI models represent a paradigm shift: They learn from examples to identify patterns humans might never recognize.[6] This capability enables agencies to:

1. **Process unstructured data:** Convert millions of pages of text, images, or audio into actionable intelligence
2. **Identify hidden patterns:** Detect fraud, security threats, or system failures before they manifest
3. **Scale human expertise:** Apply specialist knowledge across millions of cases simultaneously
4. **Predict future states:** Forecast resource needs, maintenance requirements, or emerging risks

1 National Security Commission on Artificial Intelligence, The Final Report (Washington, DC: National Security Commission on Artificial Intelligence, 2021).

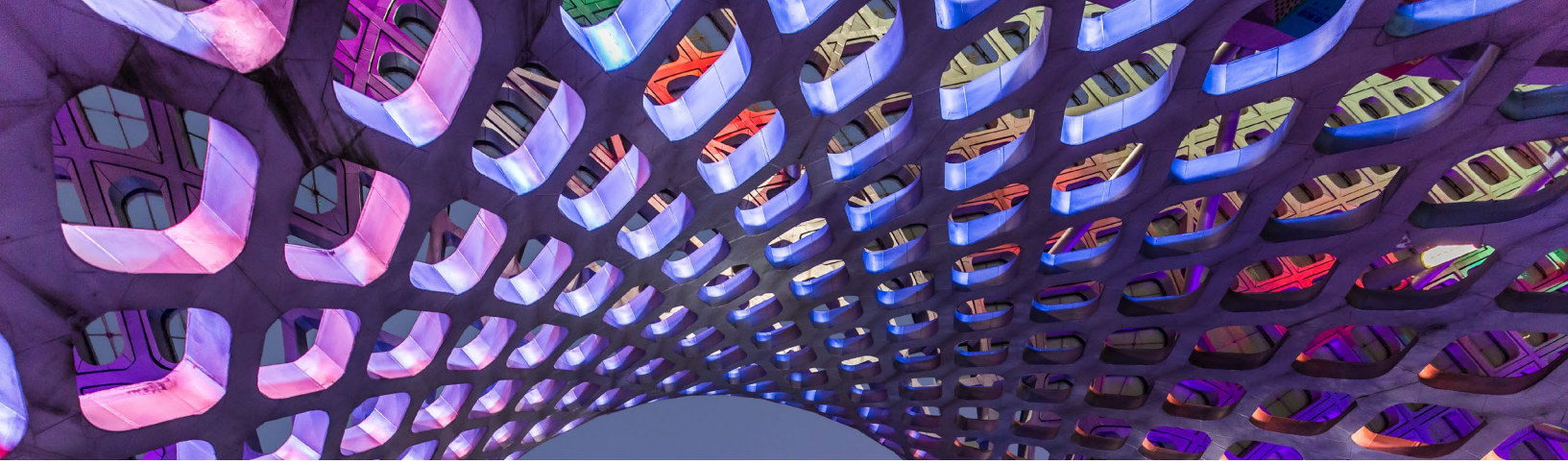
2 U.S. Government Accountability Office, Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements, GAO-24-105980 (Washington, DC: U.S. Government Accountability Office, 2023).

3 Executive Office of the President, "Removing Barriers to American Leadership in Artificial Intelligence," Executive Order 14179, The White House, January 23, 2025.

4 National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Gaithersburg, MD: National Institute of Standards and Technology, 2023).

5 Executive Office of the President, "Removing Barriers to American Leadership in Artificial Intelligence."

6 National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework.



Types of AI Models Relevant to Federal Operations

Different agency missions require different AI approaches. Understanding these categories helps leaders make informed investment decisions:[7]

1 Foundation Models

Large, general-purpose models trained on vast datasets (such as GPT-4, Claude, and Gemini): These models can be adapted for multiple tasks without retraining. Agencies use foundation models for document analysis, report generation, and citizen services. Cost: $10 million–$100 million to develop, $1,000–$10,000 per month to operate.

2 Sovereign Models

AI models developed and controlled entirely within U.S. government infrastructure, addressing national security requirements and reducing dependency on foreign-controlled commercial systems.[8] These models operate within federal security boundaries, ensuring data sovereignty and compliance with classification requirements. Critical for defense, intelligence, and sensitive civilian applications where foreign influence or data exfiltration risks are unacceptable.

3 Commercial Models

Commercially developed AI solutions available through vendor licensing or cloud services. These offer rapid deployment and proven capabilities but require careful evaluation of data handling practices, security controls, and potential dependencies on foreign infrastructure or ownership.[9] Federal procurement should prioritize vendors with FedRAMP authorization and transparent supply chain documentation.

4 Specialized Models

Purpose-built models for specific tasks (image recognition, language translation, anomaly detection): These offer superior performance for narrow applications. Example: TSA's threat detection models process millions of x-ray images daily. Cost: $100,000–$5 million to develop, $100–$1,000 per month to operate.

5 Fine-Tuned Models

Foundation models adapted with agency-specific data: These combine broad capabilities with domain expertise. Example: VA's medical diagnosis assistant trained on veteran health records. Cost: $10,000–$500,000 to develop, similar operating costs to foundation models.

6 Agency-Specific Models

Custom models designed and trained specifically for an agency's unique mission requirements and operational environment.[10] These provide maximum control over model behavior, security, and compliance but require significant investment in data infrastructure, technical talent, and ongoing maintenance. Ideal for agencies with highly specialized requirements that commercial or shared federal solutions cannot address.

7 Edge Models

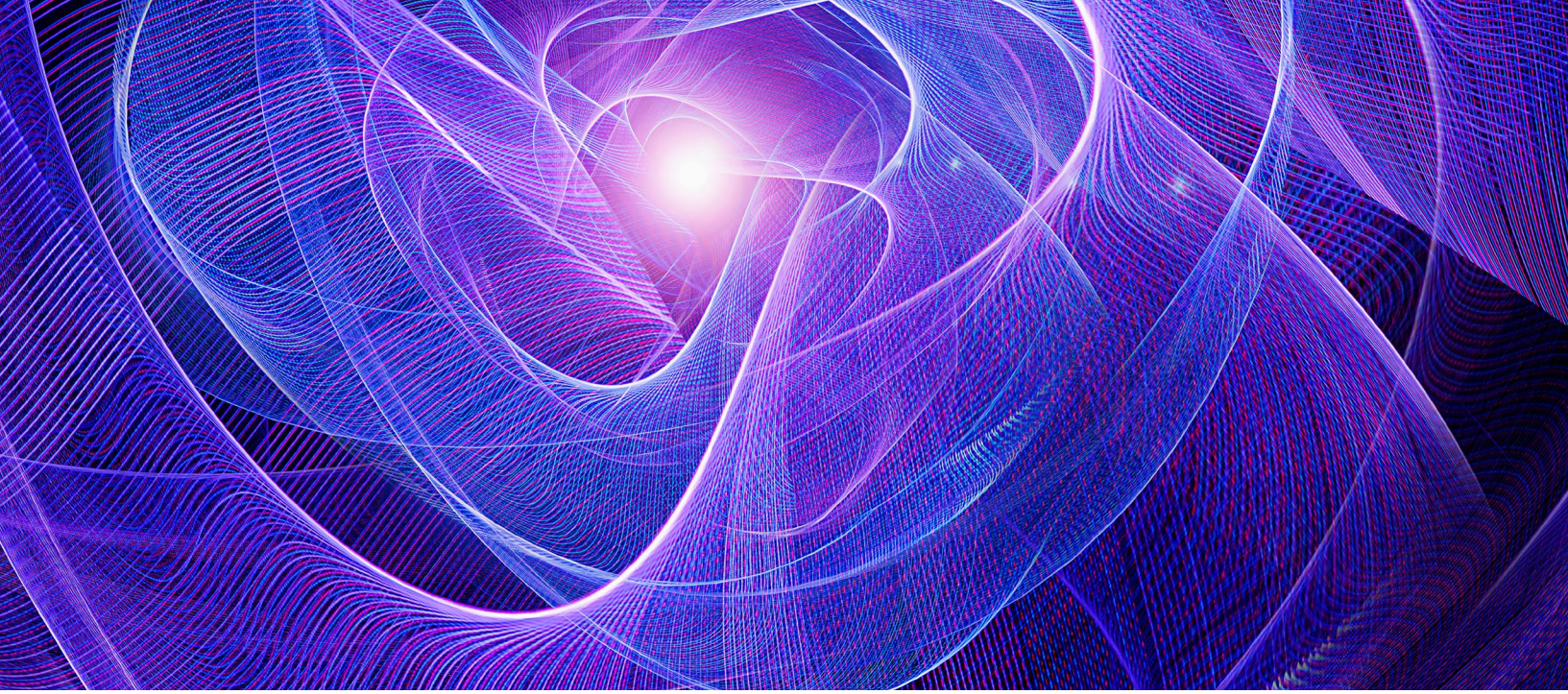
Lightweight models that run on local devices without cloud connectivity: Critical for classified environments or field operations. Example: DoD's offline translation devices for deployed personnel. Cost: $50,000–$500,000 to develop, minimal operating costs.

7 U.S. Department of Defense, DoD Data, Analytics, and Artificial Intelligence Adoption Strategy (Washington, DC: U.S. Department of Defense, November 2, 2023).

8 National Security Commission on Artificial Intelligence, The Final Report.

9 U.S. Government Accountability Office, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities, GAO-21-519SP (Washington, DC: U.S. Government Accountability Office, 2021).

10 U.S. Department of Defense, DoD Data, Analytics, and Artificial Intelligence Adoption Strategy.



Model Architecture Design Considerations

Agencies must consider architectural decisions that impact model performance, security, and maintainability:[11]

Standardized Model Context Protocols:

Establish consistent interfaces for how models receive inputs, process data, and deliver outputs across agency systems. Standardization enables interoperability, reduces integration costs, and facilitates model sharing across the federal enterprise.

Model Drift Management:

AI models degrade over time as the data they encounter diverges from their training data. Agencies must implement continuous monitoring to detect performance degradation and establish retraining protocols to maintain model accuracy and reliability.[12]

Validation and Verification:

AI ideally produces consistent outputs for consistent inputs, but poorly trained or validated AI can introduce unacceptable variability. Agencies must complete rigorous testing and validation before deployment to ensure models perform reliably across expected operating conditions.[13]

Understanding Model Capabilities and Limitations

Agency leaders must understand both what AI models can and cannot do:[14]

What AI Models Excel At:

- Pattern recognition across massive datasets
- Consistent application of complex criteria
- 24/7 operation without fatigue
- Multi-language and multi-modal processing
- Rapid scaling across geographic regions

Critical Limitations to Consider:

- Cannot explain reasoning in legally sufficient detail for all decisions
- May perpetuate biases present in training data
- Require substantial computing resources and energy
- Performance degrades with data drift over time
- Vulnerable to adversarial attacks and data poisoning[15]

11 National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework.

12 U.S. Government Accountability Office, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities.

13 National Institute of Standards and Technology, NIST AI 100-2 E2025: Adversarial Machine Learning (Gaithersburg, MD: National Institute of Standards and Technology, March 24, 2025).

14 National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework.

15 National Institute of Standards and Technology, NIST AI 100-2 E2025: Adversarial Machine Learning.

Key Distinctions for Legal and Compliance Review

- **AI Models** are the core analytical engines—the algorithms and parameters that process information
- **AI Systems** encompass the complete operational environment, including data pipelines, security controls, and monitoring capabilities
- **AI Applications** are the user-facing tools that agency personnel interact with daily[16]

This distinction matters for procurement, risk assessment, and compliance. When evaluating AI initiatives, agencies must consider all three layers to ensure comprehensive governance.

The Federal AI Challenge

Federal agencies operate on 18–24 month timelines, but AI evolves every 6–12 months, creating significant risks to capability and competitive advantage.

Traditional federal IT procurement and deployment cycles cannot accommodate AI's rapid evolution.[17] Agencies typically operate on 18–24 month implementation timelines, while AI capabilities advance significantly every 6–12 months. This misalignment creates three critical risks:

- **Capability Gap:** Agencies deploy outdated technology while adversaries leverage cutting-edge capabilities[18]
- **Talent Drain:** Top AI talent gravitates toward organizations with modern tools and agile processes[19]
- **Mission Impact:** Citizens receive suboptimal services while agencies struggle with legacy approaches[20]

Current Challenges Facing Federal AI Adoption

Federal agencies face multifaceted challenges that extend far beyond technical implementation. According to GAO reports, agencies pursuing AI innovation face critical challenges including infrastructure fragmentation across uncoordinated efforts, absence of standardized evaluation frameworks, dependency on commercial models requiring careful security evaluation, and limited operational experience in AI governance.[21]

Leadership teams struggle to balance innovation mandates with risk management responsibilities. CIOs report that traditional IT governance frameworks prove inadequate for AI's probabilistic nature and rapid evolution.[22] The human dimension presents equally significant challenges: agencies compete for scarce AI talent against private sector compensation packages significantly higher than government scales, and time-to-hire for specialized AI roles often exceeds private sector timelines by months.[23]

16 Office of Management and Budget, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Memorandum M-24-10, March 28, 2024.

17 U.S. Government Accountability Office, Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements.

18 National Security Commission on Artificial Intelligence, The Final Report.

19 U.S. Office of Personnel Management, Skills-Based Hiring Guidance and Competency Model for Artificial Intelligence Work (Washington, DC: U.S. Office of Personnel Management, April 29, 2024).

20 U.S. Government Accountability Office, Artificial Intelligence: Generative AI Use and Management at Federal Agencies, GAO-25-107653 (Washington, DC: U.S. Government Accountability Office, 2025).

21 Ibid.

22 U.S. Government Accountability Office, Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements,

23 U.S. Office of Personnel Management, Skills-Based Hiring Guidance and Competency Model for Artificial Intelligence Work.

2. FEDERAL REQUIREMENTS AND RESOURCES

To enable compliance with federal requirements, Congress has allocated significant resources to support agency AI adoption.

Evolving Regulatory Landscape

Agency counsel and leadership must navigate an evolving regulatory landscape. In January 2025, Executive Order 14179, "Removing Barriers to American Leadership in Artificial Intelligence," signaled a shift in federal AI policy toward promoting innovation while maintaining appropriate safeguards.[24] This order directs agencies to sustain and enhance America's global AI dominance while promoting human flourishing, economic competitiveness, and national security.

Current requirements and guidance include:

- **NIST AI Risk Management Framework (AI RMF 1.0):** Establishes voluntary standards for AI system evaluation and monitoring through four core functions: Govern, Map, Measure, and Manage[25]
- **Chief AI Officer Requirements:** Federal agencies maintain designated CAIOs responsible for coordinating AI governance and innovation[26]
- **AI Use Case Inventories:** Agencies continue to report AI use cases, with over 1,700 use cases reported as of December 2024[27]
- **GAO AI Accountability Framework:** Provides key practices for ensuring accountability and responsible AI use organized around governance, data, performance, and monitoring principles[28]

Available Federal Resources

Congress has authorized significant resources to support agency AI adoption:

- **National AI Research Resource (NAIRR) Pilot:** Launched in January 2024, this public-private initiative provides access to computational resources, datasets, models, software, training, and user support. As of late 2024, the NAIRR Pilot has made over 150 resource awards supporting research and education across the nation.[29]
- **Federal AI Training Resources:** OPM and agency-specific training programs for federal employees at all levels[30]
- **Interagency AI Collaboration:** The Chief AI Officers Council and related interagency bodies facilitate resource sharing and best practice exchange[31]

24 Executive Office of the President, "Removing Barriers to American Leadership in Artificial Intelligence."

25 National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework.

26 Office of Management and Budget, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

27 CIO Council, "Consolidated 2024 Federal AI Use Case Inventory," CIO.gov, 2024.

28 U.S. Government Accountability Office, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities.

29 National Science Foundation, "National Artificial Intelligence Research Resource (NAIRR) Pilot," 2024.

30 U.S. Office of Personnel Management, Skills-Based Hiring Guidance and Competency Model for Artificial Intelligence Work.

31 Office of Management and Budget, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

3. BUILDING YOUR AGENCY'S AI PROGRAM

An agency's AI infrastructure builds on a bedrock of governance, technical capabilities, and organizational culture.

Establishing a successful AI program requires more than technology acquisition. Agencies must create an ecosystem that supports innovation while maintaining security, compliance, and public trust.[32] This section provides detailed guidance on building the organizational, technical, and cultural foundations for AI success.

Governance Structure: The Foundation of AI Success

Effective AI governance balances innovation with oversight. Agencies should establish a three-tier structure that separates strategic direction, operational management, and technical evaluation:[33]

1. Executive AI Board

Chaired by the Deputy Secretary or equivalent, this board provides strategic direction and resource allocation. Members should include the CIO, CFO, General Counsel, and mission area leaders.

Key Responsibilities:

- Approve AI strategy and investment priorities
- Allocate resources across competing initiatives
- Review high-risk AI deployments
- Ensure alignment with agency mission and values
- Report to agency head on AI progress and risks

Meeting Cadence: Monthly initially, quarterly once established. Emergency sessions for critical incidents or major deployments.

2. Chief AI Officer (CAIO)

This role coordinates AI initiatives across the agency. The position should report directly to agency leadership (the agency head or their deputy) and have budget authority.[34] The CAIO serves as the central point of accountability for AI outcomes.

Essential Qualifications:

- Senior Executive Service (SES) or equivalent level
- Direct report to agency head or deputy
- Budget authority for AI initiatives
- Technical understanding of AI capabilities and limitations
- Experience managing complex technology programs

3. AI Review Board

A technical body that evaluates AI systems for safety, security, and compliance. Include representatives from IT, security, privacy, and civil rights offices. This board provides independent technical assessment separate from business advocacy.

32 U.S. Government Accountability Office, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities.

33 Office of Management and Budget, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."

34 Ibid.

Risk-Based Implementation Approach

Not all AI applications carry equal risk. Agencies should categorize initiatives to allocate oversight resources efficiently.[35] This tiered approach accelerates low-risk deployments while ensuring appropriate scrutiny for high-impact systems.

Low-Risk Applications (Streamlined Approval)

Administrative automation, document summarization, and internal analytics. These can proceed with streamlined approval processes.

Examples:

- Meeting transcription and summarization
- Document classification and routing
- Internal knowledge management
- Code review and documentation
- Help desk ticket triage

Medium-Risk Applications (Standard Review)

Decision support systems, predictive maintenance, and operational optimization. Require documented testing and monitoring protocols. Examples include budget forecasting models, equipment failure prediction, workforce planning tools, and supply chain optimization.

High-Risk Applications (Comprehensive Review)

Systems affecting individual rights, benefits determinations, or law enforcement. Mandate comprehensive impact assessments and continuous oversight.[36] Examples include benefits eligibility determination, security clearance adjudication, law enforcement risk assessment, and medical diagnosis or treatment recommendations.

Partnership Strategy: Accelerating Through Collaboration

Agencies cannot build all AI capabilities in-house; strategic partnerships drive faster implementation and mitigate risks.

No agency can develop all AI capabilities internally. Strategic partnerships accelerate implementation while managing risk.[37] Successful agencies leverage four types of partnerships:

1. **Federally Funded Research and Development Centers (FFRDCs)**
   Provide independent validation and specialized expertise without commercial conflicts of interest. Engage for high-risk system validation, classified or sensitive applications, cross-agency initiatives, and technology assessment and forecasting.

2. **Academic Institutions**
   Offer research capabilities, talent pipeline, and cutting-edge innovation through Cooperative Research and Development Agreements (CRADAs), grant-funded research programs, student internship pipelines, and faculty advisory boards.

3. **Industry Partners**
   Deliver proven solutions and implementation expertise through Other Transaction Agreements (OTAs) for prototypes, challenge competitions and prizes, Commercial Solutions Openings (CSOs), and modular contracting for rapid iterations.

4. **Other Federal Agencies**
   Enable resource sharing and best practice exchange through Interagency Agreements (IAAs), joint task forces, shared service providers, and communities of practice.

35 U.S. Government Accountability Office, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities.

36 CIO Council, "Consolidated 2024 Federal AI Use Case Inventory."

37 National Science Foundation, "National Artificial Intelligence Research Resource (NAIRR) Pilot."

Technical Infrastructure: Building the Foundation

AI systems require robust technical infrastructure that goes beyond traditional IT. Agencies must address five critical components:

1 Data Management

AI models are only as good as their training data. Agencies must establish:

- Data governance frameworks defining ownership and usage rights
- Quality assurance processes for accuracy and completeness
- Bias detection and mitigation procedures
- Privacy-preserving techniques (differential privacy, federated learning)
- Version control and lineage tracking

2 Computing Resources

AI workloads demand specialized computing infrastructure:

- GPU clusters for model training
- Edge computing for real-time inference
- Elastic scaling for variable workloads
- Hybrid cloud architectures for flexibility
- Disaster recovery and continuity planning

3 Security Controls

AI systems introduce unique security challenges:

- Model theft and reverse engineering protection
- Adversarial attack detection and prevention
- Data poisoning safeguards
- Supply chain security for AI components
- Zero-trust architectures for model access

4 Monitoring Systems

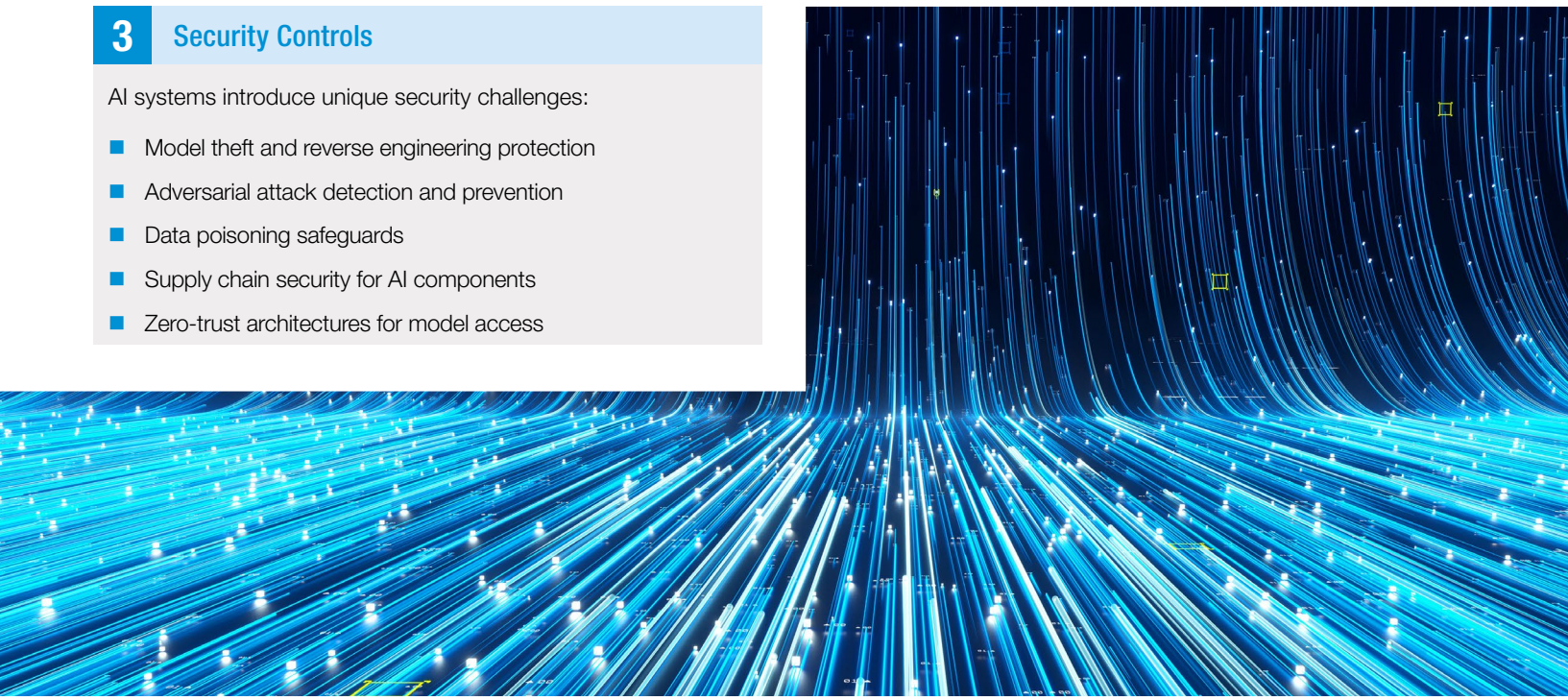
Continuous monitoring ensures AI systems perform as intended:

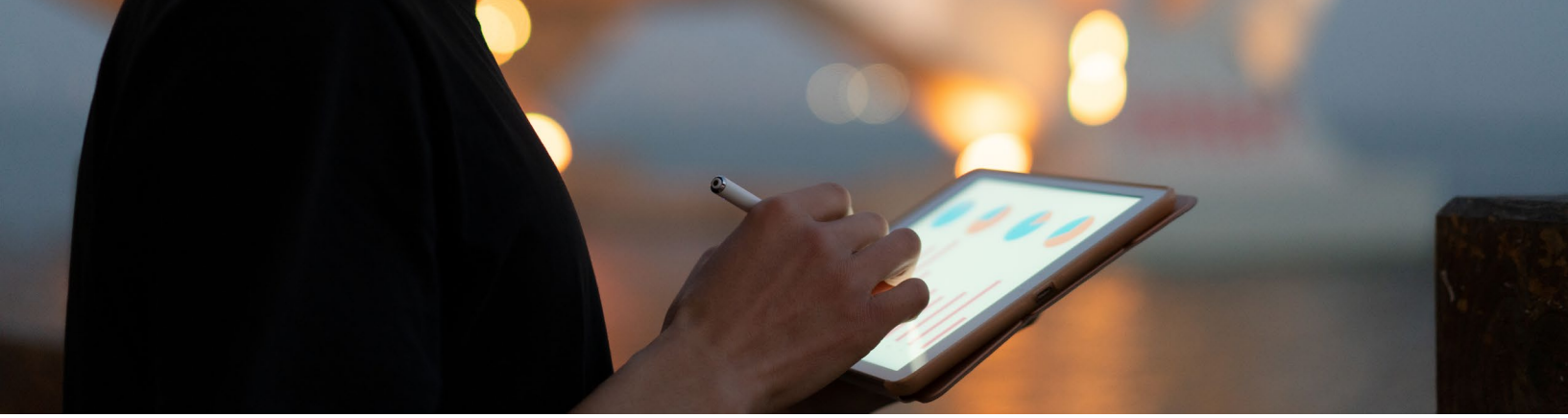
- Performance metrics dashboards
- Drift detection algorithms
- Fairness and bias monitoring
- Explainability tools for decision auditing
- Automated alerting for anomalies

5 Integration Capabilities

AI must work within existing agency systems:

- API gateways for secure access
- Message queuing for asynchronous processing
- Legacy system adapters
- Data transformation pipelines
- Workflow orchestration tools





4. IMPLEMENTATION ROADMAP

Foundation (Months 1–3)

Phase 1

Establish governance and assess current state:[38]

1. Designate Chief AI Officer and establish AI governance boards
2. Inventory existing AI initiatives and identify capability gaps
3. Assess data readiness and identify high-value datasets
4. Review legal authorities and update procurement vehicles
5. Engage NAIRR and interagency resources for support[39]

Pilot (Months 4–9)

Phase 2

Launch initial projects and build capabilities:

1. Select 2–3 low-risk, high-value use cases for pilot implementation
2. Establish testing protocols and success metrics[40]
3. Deploy initial AI tools using authorized solutions
4. Begin workforce training through available federal programs[41]
5. Develop agency-specific AI policies and procedures

Scale (Months 10–18)

Phase 3

Expand successful initiatives and build advanced capabilities:

1. Scale proven use cases across the enterprise
2. Develop custom models for mission-specific requirements[42]
3. Implement continuous monitoring and improvement systems[43]
4. Establish interagency partnerships for resource sharing
5. Deploy citizen-facing AI services with appropriate safeguards

38 Office of Management and Budget, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
39 National Science Foundation, "National Artificial Intelligence Research Resource (NAIRR) Pilot."
40 National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework.
41 U.S. Office of Personnel Management, Skills-Based Hiring Guidance and Competency Model for Artificial Intelligence Work.
42 U.S. Department of Defense, DoD Data, Analytics, and Artificial Intelligence Adoption Strategy.
43 U.S. Government Accountability Office, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities.

5. LEGAL AND COMPLIANCE CONSIDERATIONS

To enable compliance with federal requirements, Congress has allocated significant resources to support agency AI adoption.

Key Legal Requirements

Agency counsel must ensure AI implementations comply with existing statutory and regulatory frameworks:

- **Administrative Procedure Act:** AI-assisted decisions must maintain transparency and reviewability
- **Privacy Act:** Systems of records notices may require updates for AI data processing
- **Federal Records Act:** AI-generated content and decision logs must be properly retained
- **Section 508:** AI interfaces must meet accessibility standards
- **Constitutional Protections:** Due process and equal protection considerations for automated decisions

Procurement Considerations

AI procurement demands innovative contracting approaches, including modular designs, performance-based requirements, IP negotiations, vendor transparency, and clear liability terms.

AI procurement requires modified approaches to traditional contracting:[44]

- Use modular contracting to accommodate rapid technology changes
- Include performance-based requirements rather than prescriptive specifications
- Negotiate intellectual property rights for model improvements
- Require vendor transparency on training data and model limitations
- Establish clear liability allocation for AI-related errors

44 U.S. Government Accountability Office, Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements,

6. HOW A&M SUPPORTS FEDERAL AI TRANSFORMATION

A&M brings extensive experience helping federal agencies navigate complex transformations. Our approach combines strategic planning, technical expertise, and implementation support tailored to government requirements.

Strategic Advisory Services

- AI readiness assessments aligned with federal maturity models
- Governance framework design compliant with federal requirements
- Risk management strategies based on NIST frameworks
- Business case development for Congressional justifications

Implementation Support

- Program management for AI initiatives
- Technical architecture design and validation
- Vendor evaluation and selection support
- Change management and workforce development

Compliance and Risk Management

- Legal and regulatory compliance reviews
- Security control implementation and validation
- Audit preparation and response support
- Continuous monitoring system design

A&M measures success by the lasting impact of our work on agency performance and public service delivery.

Contact A&M's Federal AI Practice to discuss how we can accelerate your agency's AI transformation while ensuring compliance and managing risk.

About Alvarez & Marsal

Alvarez & Marsal delivers results when it really matters. With over 11,000 professionals across five continents, we provide leadership, action, and results to government and commercial clients facing complex challenges.

Our Federal practice combines deep government expertise with proven private sector approaches. We help agencies transform operations, implement new technologies, and achieve mission objectives within regulatory constraints.

A&M operates as a trusted advisor to federal leaders, providing independent, objective guidance backed by hands-on implementation support. We measure success by the lasting impact of our work on agency performance and public service delivery.

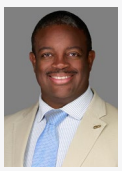
REFERENCES

1. Executive Office of the President, "Removing Barriers to American Leadership in Artificial Intelligence," Executive Order 14179, The White House, January 23, 2025.
2. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Gaithersburg, MD: National Institute of Standards and Technology, 2023).
3. U.S. Department of Defense, DoD Data, Analytics, and Artificial Intelligence Adoption Strategy (Washington, DC: U.S. Department of Defense, November 2, 2023).
4. Office of Management and Budget, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Memorandum M-24-10, March 28, 2024.
5. U.S. Government Accountability Office, Artificial Intelligence: Generative AI Use and Management at Federal Agencies, GAO-25-107653 (Washington, DC: U.S. Government Accountability Office, July 29, 2025).
6. U.S. Government Accountability Office, Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements, GAO-24-105980 (Washington, DC: U.S. Government Accountability Office, December 12, 2023).
7. U.S. Government Accountability Office, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities, GAO-21-519SP (Washington, DC: U.S. Government Accountability Office, 2021).
8. National Science Foundation, "National Artificial Intelligence Research Resource (NAIRR) Pilot," 2024.
9. CIO Council, "Consolidated 2024 Federal AI Use Case Inventory," CIO.gov, 2024.
10. National Security Commission on Artificial Intelligence, The Final Report (Washington, DC: National Security Commission on Artificial Intelligence, 2021).
11. U.S. Office of Personnel Management, Skills-Based Hiring Guidance and Competency Model for Artificial Intelligence Work (Washington, DC: U.S. Office of Personnel Management, April 29, 2024).
12. National Institute of Standards and Technology, NIST AI 100-2 E2025: Adversarial Machine Learning (Gaithersburg, MD: National Institute of Standards and Technology, March 24, 2025).

KEY CONTACTS

Edward Hanapole
Public Sector Services
Managing Director and Chief AI Officer

ehanapole@alvarezandmarsal.com



Louverture Jones
National Security, Trade & Technology
Senior Director

louverture.jones@alvarezandmarsal.com

Follow A&M on:

477460-55553/February 26
9917_Stg02

ABOUT ALVAREZ & MARSAL

Founded in 1983, Alvarez & Marsal is a leading global professional services firm. Renowned for its leadership, action and results, Alvarez & Marsal provides advisory, business performance improvement and turnaround management services, delivering practical solutions to address clients' unique challenges. With a world-wide network of experienced operators, world-class consultants, former regulators and industry authorities, Alvarez & Marsal helps corporates, boards, private equity firms, law firms and government agencies drive transformation, mitigate risk and unlock value at every stage of growth.

To learn more, visit: **AlvarezandMarsal.com**

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.℠