DATA AND AI REPORT

Foundations, Frontiers, and Fault Lines

A 12-Month Look Forward Into the Federal Data and AI Landscape

By Stephen Erickson, Matthew McDonald, Patrick Elder, Ketan Mane, Ph.D., and Mojgan Pedoeim

V090525

Table of Contents

Introduction

This report will arm federal leaders, mission owners, and technologists with a clear-eyed, forward-looking view of what matters most for data and artificial intelligence in the year ahead. Structured around foundational imperatives ("foundations"), emerging trends ("frontiers"), and real-world risks ("fault lines"), it highlights the ***key shifts and strategic pivots agencies must make*** *to achieve lasting impact with their data and AI investments.*

From Incremental Change to Mission Transformation

Data and AI are reshaping federal operations, moving beyond small improvements to profound mission transformation. From empowering warfighters with geospatial intelligence (GEOINT) AI to anticipating fraud, optimizing supply chains, and prioritizing veteran claims, data and AI tools can **accelerate mission outcomes and elevate service quality**.

This shift is already well underway. Federal spending on data infrastructure and AI surged from 2021 to 2023, spurred by the 2018 Evidence Act and reinforced by recent Executive Orders and Office of Management and Budget (OMB) memoranda that institutionalized data-driven policymaking. AI is now a federal priority, fueling growth by design rather than chance.

By 2031, the federal AI market is projected to reach nearly $60 billion, growing at a 15.8% compound annual growth rate (CAGR). Defense agencies still lead investment, but civilian agencies are catching up, with directives **pushing workflow automation and procurement modernization**. The government's AI Action Plan also calls for **removing regulations** that hinder AI adoption.

Challenges on the Horizon

Despite clear momentum, challenges remain. Many agencies rely on legacy systems that limit scalability, and AI pilots often stall when early use cases show limited impact. Competition for AI talent is also fierce, as commercial sectors offer **faster career progression, more flexible environments, and higher pay.**

Building and scaling effective, ethical, and secure AI is hard work. Success requires not only modernization, but also **cultural alignment, robust governance, and thoughtful policy navigation**. The urgency is real, but so are the hurdles.

[1] InsightAce Analytic

Foundations

These are the non-negotiable capabilities and conditions necessary for data and AI success.

1. Responding to Advancing AI Ecosystems

The U.S. government is not only ramping up investments in AI, but also restructuring how those investments are governed. This includes the formal appointment of Chief AI Officers (CAIOs), the creation of cross-agency governance boards, and the introduction of frameworks to **promote innovation while managing risk**.

This is not a symbolic move — it's a structural one. In the coming year, the push for global AI leadership will continue to reshape the federal AI ecosystem. Agencies must **continuously evaluate how their initiatives support the broader mission** of U.S. innovation and competitiveness.

Take the next steps:

- Identify and prioritize **mission-specific use cases** to ensure AI delivers tangible value across diverse missions.
- Demonstrate **adaptive strategies** aligned with national priorities such as cybersecurity, economic competitiveness, and public trust.
- Leverage flexible AI playbooks that integrate both **federal and commercial solutions**, recognizing that many products require customization and governance to deliver sustainable outcomes.
- Highlight concrete innovation examples — from GEOINT for operational decision-making to healthcare AI for claims processing — that illustrate AI's cross-sector impact.

To maximize impact, agencies must move from broad strategies to mission-specific use cases where AI can deliver measurable outcomes. Success will depend not only on the technology itself, but on how well it integrates with existing workflows and serves the people who will use and govern it.

To operationalize this shift, agencies must advance beyond isolated pilots and build **mission-ready, actionable AI ecosystems**. That means scaling talent pipelines, creating shared model repositories, and accelerating collaboration across agencies, academia, and industry. By doing so, government can ensure that AI adoption is not just widespread, but sustainable and strategically aligned.

> Collaboration will be critical to ensuring the U.S. remains at the forefront of **responsible, secure, and globally competitive AI deployment**.

Foundations

2. Implementing Scalable, Mission-aligned Data Governance

AI is only as effective as the data that feeds it. As federal agencies collect and share more data across systems, missions, and classifications, **the need for robust governance becomes mission critical**. Poor data governance can erode public trust, produce unreliable insights, and even introduce unintentional bias or discrimination.

At the heart of this challenge is the need to **balance accessibility with control**. Data mesh and data fabric architectures offer potential solutions, enabling decentralized access to data while maintaining centralized oversight and security. But implementing these concepts requires significant cultural and technical change. Agencies can also use the Model Context Protocol (MCP) to standardize data understanding. Finally, agentic mesh (an interconnected network of autonomous software agents) enables decentralized, policy-driven decision making. Together, these approaches support adaptive, responsive governance.

Take the next steps:

- Elevate data governance to a strategic priority, embedding it across policy, technology, and workforce practices.
- Treat governance as an enabler, not a constraint, and ensure data is clean, trusted, and aligned with mission goals.
- Look for ways to make governance an accelerator by embedding it closer to the source.

To move from vision to execution, agencies should operationalize governance through **dynamic metadata management, automated lineage tracking, and role-based access control** that adapts to evolving missions. Embedding governance within DevSecOps pipelines through methods like Compliance as Code (CaC) and Policy as Code (PaC) ensures data quality is continuously monitored and improved. Furthermore, agencies should define cross-functional data steward roles to bridge gaps between IT, mission operators, and legal teams, ensuring governance frameworks are both technically sound and mission-aware. Agentic mesh can automate governance tasks, while MCP-based services deliver real-time insights.

In geospatial use cases, for example, robust governance is especially critical. Location-based data can be sensitive and fast-moving; combining it with AI models requires strict control over lineage, source integrity, and access. MCP improves shared spatial understanding, while agentic mesh automates data processing for faster, more accurate decisions.

> **As data sharing becomes essential to AI collaboration, scalable governance through data mesh and fabric architectures, MCP, and agentic mesh is no longer optional – it's foundational to agility, compliance, and impact.**

Foundations

3. Adapting to Rapidly Shifting Compliance and Acquisition Mandates

In April 2025, two OMB memoranda (M-25-21 and -22) introduced sweeping reforms in how federal agencies acquire, evaluate, and govern AI. These directives require agencies to build infrastructure for **rigorous testing, auditing, and monitoring of AI systems**, not just before deployment, but continuously throughout their lifecycle.

Building on these directives, the government's July 2025 AI Action Plan introduced additional priorities for accelerating responsible AI adoption. Beyond compliance, the plan emphasizes **cross-agency coordination, workforce enablement, and measurable mission outcomes**, signaling a shift toward a more integrated federal strategy for governing AI.

These rules carry teeth. Agencies must identify and mitigate risks associated with AI systems, particularly those categorized as "high impact," and submit compliance roadmaps tied to federal standards. The result is a compliance environment that demands not only technical fluency, but operational agility and clear leadership.

> Embedding compliance into daily practice will not only **prevent failures** but also **accelerate sustainable innovation** under heightened scrutiny.

Take the next steps:

- Treat compliance not as a checklist, but as an operating principle.
- Prioritize commercially available AI tools with verifiable performance histories to accelerate acquisition timelines and reduce risk.
- Establish measurable performance metrics.
- Avoid long-term vendor lock-in.
- Adhere to new procurement priorities, particularly the "Buy American" provisions that will increasingly govern technology sourcing.
- Align compliance and acquisition strategies with the priorities outlined in the AI Action Plan, particularly around workforce readiness, interagency collaboration, and responsible AI practices.

As agencies adapt, they must also strengthen internal governance frameworks to ensure accountability across multidisciplinary teams. This includes embedding compliance liaisons early in the procurement process, aligning acquisition teams with legal, cybersecurity, and data science personnel to preemptively identify friction points. Moreover, agencies should begin **developing repeatable, modular acquisition templates for AI capabilities**, enabling speed and consistency while complying with evolving mandates and ensuring new tools are interoperable rather than siloed. These templates should also drive down technical debt and include KPIs to reduce acquisition costs and timelines while supporting mission outcomes.

Frontiers

These are the emerging shifts that will shape federal data and AI strategy over the next 12 months.

1. From Generic Platforms to Mission-focused Intelligence

Many agencies have invested in large, monolithic analytics platforms, only to find that these tools fail to deliver the precision or relevance needed to drive mission outcomes. In 2025, this scattershot approach is giving way to mission-focused data and AI strategies that **emphasize direct impact over broad functionality.**

What is driving this change? Resource constraints, accountability pressures, and the growing sophistication of mission owners. Decision makers now expect AI tools that are tailored to their context; not just capable of outputting results, but **capable of producing the right insights for the right moment**.

Take the next steps:

- Evaluate whether proposed AI solutions can integrate effectively within existing ecosystems (where work happens) and include data quality, availability, and interoperability considerations.
- Co-create solutions with mission users, evaluated through measurable impact metrics, and governed by agile, user-centric workflows. (ECS has demonstrated this mission focus by embedding fielded personnel directly with users to define AI capabilities that enhance mission effectiveness, while implementing feedback loops to continuously improve models in partnership with our field cadre and users.)
- Focus on enabling the frontline, not just satisfying the back office.

Equally important is the ability to operationalize intelligence within tight decision windows. This is where agentic AI can support analysis and provide the right data context, serving as a key differentiator. Mission-focused systems must **support contextual awareness, integrate with domain-specific datasets, and operate with minimal latency**. Agencies should look to modular AI architectures that can be deployed in austere or disconnected environments, empowering field agents, analysts, and warfighters alike.

For example, GEOINT AI platforms, which enable analysts and warfighters to access real-time terrain analysis, object detection, and mission planning tools, even in denied or degraded communications environments, offer precisely this kind of agility.

> **In this next phase of AI maturity, success will depend not on how powerful a platform is in theory, but how precisely it serves those on the ground in real time.**

Frontiers

2. Speed to Impact as a Strategic Imperative

In today's dynamic threat environment, the ability to act quickly is not a luxury but a mission requirement. That means **speed to impact must become a core design principle** across the data and AI lifecycle, from procurement to deployment. Edge manufacturing, enabled by location-aware GEOINT AI platforms, is a prime example of this mindset, creating a just-in-time operational strategy with dramatically reduced logistics friction.

Recent executive directives emphasize this shift, particularly through reforms to the Federal Acquisition Regulation (FAR). Agencies are being encouraged — and in some cases, required — to **streamline acquisition cycles, adopt modular contracting approaches, and rapidly prototype emerging technologies**.

> **The goal is not just to move fast but to move smart, with decisions rooted in mission urgency and informed by continuous data.**

Take the next steps:

- Adopt lean, iterative development models that deliver real value in hours, days, and weeks, not months and years (this is where agentic automation can deliver results).
- Minimize delays at every stage: procurement, development, rollout, and training. (For example, in the realm of GEOINT, ECS' Joint Warfighter Toolbox (JWT) platform enables rapid ingestion, model execution, and workflow integration, while our Field Support Operations (FSO) team embeds analyst-engineer teams with users to ensure smooth deployment and avoid handoff delays).
- Align every step of the AI journey with a specific, measurable mission outcome.

Additionally, **embedding mission stakeholders into cross-functional AI delivery teams** from day one ensures immediate feedback loops and minimizes rework.

Frontiers

3. Operationalizing Emerging Technologies

The data and AI landscape is evolving fast. Technologies like agentic AI, multimodal models, and citizen data science platforms are rapidly changing what is possible and who can participate. Meanwhile, architectures such as data mesh and Artificial Intelligence Operations (AIOps) pipelines are **improving scale, efficiency, and reproducibility**.

But these tools don't operate in a vacuum. Their value depends on how well they are integrated into existing mission environments. Agencies must focus not only on what's new, but on what works, deploying technologies that are accessible, adaptable, and aligned with their data maturity.

Take the next steps:

- Prioritize workforce enablement, governance automation, and interoperability across systems.
- Treat emerging technologies as mission enablers, not just technical upgrades, to build and maintain strategic advantages in 2025 and beyond.
- Adopt a product mindset by understanding who the users are, their pain points, and how solutions can be embedded directly into mission workflows.

To make this real, agencies must leverage **secure, unclassified test environments for experimentation,** allowing for low-risk testing of new AI capabilities before scaling them into production. This includes establishing AIOps pipelines with embedded compliance checks, using synthetic data to accelerate model training without compromising security or privacy, and ensuring low-code/no-code tools are available to domain experts outside traditional IT.

An example of this is the operationalization of GEOINT AI, as secure sandbox environments support rapid experimentation with satellite, drone, and sensor data to train geospatial models before deployment to mission environments.

The key to operationalizing innovation is leveraging secure-but-accessible environments that make it possible to develop and deploy effective technologies at speed and scale.

Fault Lines

These are the operational, structural, and strategic risks that can derail data and AI efforts.

1. Lack of a Unified Strategy

Without a coherent data and AI strategy, even the best-intentioned projects falter. Agencies that treat AI as a bolt-on capability, rather than an integrated mission asset, will struggle to scale, govern, or secure their initiatives.

The absence of strategy often leads to fragmented efforts, overlapping investments, and poor alignment with agency goals. It also leaves critical gaps in governance, particularly around responsible AI, data privacy, and system reliability.

Over the next year, strategic clarity will be the difference between experimentation and transformation.

Take the next steps:

- Develop enterprise-wide roadmaps that tie AI to outcomes, risks, and resources.
- Drive automation to accelerate tasks.
- Continuously iterate as the landscape evolves.

That clarity must be reinforced through visible executive sponsorship and cross-functional alignment. Agencies should designate accountable AI stewards at the mission level and link strategy to existing performance management frameworks. Strategic planning should also include a clear inventory of current AI capabilities, integration points with legacy systems, and metrics for maturity assessment, with continuous monitoring to ensure that data and application integrations remain **scalable, governable, and secure**.

Without a unified vision that bridges technical, operational, and policy domains, even the most advanced AI investments risk becoming isolated pilots with limited value.

Fault Lines

2. Inadequate Infrastructure

Building and maintaining the infrastructure to support data and AI is expensive and complex. Many agencies still rely on legacy systems that limit flexibility and scalability. Cloud adoption, while helpful, introduces its own challenges, especially around cost control (government spending on cloud computing is expected to exceed $30 billion by FY2028)[2] and performance optimization.

Rising cloud and compute costs are likely to become a limiting factor. Agencies will be tasked with making difficult judgment calls about **resource allocation, evaluating hybrid architectures, efficient compute models, and the long-term ROI** of different technology stacks.

Take the next steps:

- Modernize infrastructure incrementally.
- Align technology investments with mission priorities.
- Anticipate operational costs, not just capital expenses.

To address these challenges, agencies should adopt infrastructure-as-code and automated provisioning strategies to reduce configuration drift and speed up deployments. Investment should focus not just on hardware or cloud platforms, but on **building resilient data pipelines and edge-ready systems** capable of operating in bandwidth-constrained or disconnected environments. Agencies should also monitor resource utilization, such as tracking CPU, GPU, and memory usage, to identify potential performance bottlenecks and ensure infrastructure efficiency. This is particularly true for GEOINT operations and tactical manufacturing, where edge-ready infrastructure determines whether insights (or replacement parts) are delivered in time to impact the mission.

By integrating real-time observability tools, agencies can make smarter, usage-driven decisions that scale infrastructure with mission needs.

[2] Deltek Federal Cloud Computing Market, 2024-2028 report

Fault Lines

3. Trustworthy Data and System Security

As AI systems grow more powerful, the consequences of compromised data become more severe. Data poisoning, model inversion attacks, large language model (LLM) hallucinations, and privacy breaches are no longer theoretical — they are happening now. Federal agencies must treat data and AI system integrity as a national security priority.

Trustworthy data is about more than encryption or access controls. It's about **provenance, governance, and transparency**. The integrity of our decisions and the trust of the American public depend on getting this right.

Every AI system must:

- Be grounded in high-quality, bias-mitigated, securely sourced data, with continuous processes to identify and resolve quality issues and to improve collection practices upstream so that downstream AI products are more accurate and reliable.
- Be auditable, explainable, and continuously monitored.
- Implement data anonymization, ensuring data is anonymized before being used with AI services to protect user privacy and comply with legal standards.

To uphold this standard and minimize data exposure, agencies must embed zero trust principles across the AI lifecycle, validating every user, device, and dataset before granting access. Security teams should leverage threat-informed Machine Learning Operations (MLOps) frameworks that incorporate red-teaming, adversarial testing, and automated anomaly detection. Additionally, provenance tagging and immutable audit trails will be essential for tracing model behavior and **ensuring accountability during high-stakes decisions**.

> In a threat landscape defined by speed and sophistication, security must scale as aggressively as innovation – and data quality must be elevated as a first-order priority for **ensuring trustworthy outcomes**.

Fault Lines

4. The Persistent AI Talent Gap

Federal agencies are struggling to hire and retain the data and AI talent they need. In many cases, skilled candidates are lured to the private sector by higher salaries, faster innovation cycles, and greater autonomy. Those who stay often face slow-moving promotion paths and limited professional development.

Solving this challenge requires a cultural shift. Agencies will benefit from creating environments where AI professionals feel they can grow, contribute, and lead.

Take the next steps:

- Develop better pathways for upskilling existing employees.
- Partner with academic institutions.
- Implement innovative hiring models that attract non-traditional talent.

Agencies should also **reframe AI roles as mission-critical**, not just technical positions, and embed them directly within program teams instead of isolating them in IT silos. Expanding fellowships, term-limited appointments, and cross-sector exchange programs can help infuse fresh expertise into government while allowing private sector professionals to contribute without long-term career disruption.

Cultivating purpose-driven work cultures – where AI professionals observe tangible impact and experience leadership trust – creates a compelling environment for attracting and retaining top talent.

Conclusion

The future of federal government operations will be shaped by how well agencies embrace, integrate, and govern data and AI. But success will not come from technology alone. It will come from leadership: from strategic vision, bold execution, and the ability to adapt in an AI landscape that is evolving faster than ever.

The time for cautious pilot programs is over. The next 12 months will demand urgency, clarity, and accountability around AI adoption and implementation. Whether you're designing policy, supporting the warfighter, or improving citizen services, the question is the same: how will your data and AI strategy deliver **measurable, trustworthy, and mission-aligned impact**?

At ECS, we stand ready to help you answer that question.

If you have questions about the information in this report or if you want to learn more about how ECS delivers AI-fueled data insights and advanced AI/ML solutions for federal civilian and defense agencies, please contact us. We also invite you to connect with us on LinkedIn.

Stephen Erickson
Vice President, Strategic Solutions

Matthew McDonald
Senior Director, Defense and Intel

Patrick Elder
Director, Atlas Product

Ketan Mane, Ph.D.
Director, Digital and Artificial Intel Solutions

Mojgan Pedoeim
Director, Solutions Architecture

ECStech.com