SpencerFane®

The "Genesis Mission" Executive Order: AI as Strategic Advantage and What It Means for Your Business

On November 24, 2025, President Trump signed an Executive Order, Launching the Genesis Mission, which establishes a national effort to use artificial intelligence to accelerate scientific discovery and strengthen U.S. capabilities in key technology domains.

Substantively, it places AI where nuclear technology sat during the Cold War: at the center of long-term strategic competition. The opening sections frame AI as a race for "global technology dominance" and liken the initiative to the Manhattan Project in urgency and ambition. The underlying purpose is to position the U.S. as strongly as possible to prevail in a decades-long technological "cold war" over AI capability:

The Genesis Mission charges the Secretary of Energy with leveraging our National Laboratories to unite America's brightest minds, most powerful computers, and vast scientific data into one cooperative system for research (Genesis Mission Fact Sheet).

For business leaders, this is not just a science story. It is a signal about where the federal government is heading with AI – and how that direction will influence capital allocation, supply-chain expectations, and governance standards in critical sectors.

What the Genesis Mission Actually Does

The Executive Order establishes the Genesis Mission as a "national effort to accelerate the application of AI for transformative scientific discovery focused on pressing national challenges." Instead of having AI initiatives scattered across federal agencies, it directs the government to build a shared AI platform, plug in decades of federally funded scientific data, and deploy foundation models and AI

agents to speed research and experimentation.

Three structural elements matter from a business vantage point.

First, the mission is purposefully designed to focus on defined national priorities. Within 60 days, the Secretary of Energy must identify at least 20 science and technology challenges of national importance in areas such as advanced manufacturing, biotechnology, critical materials, nuclear fission and fusion, quantum information science, and semiconductors and microelectronics. These are the sectors where many businesses will either compete directly or supply key components and services.

Second, the program is dynamic. The challenge list must be reviewed and updated annually based on progress, emerging needs, and administration research priorities. That gives business leaders a recurring indicator of where federal AI priorities, funding, and regulatory scrutiny are likely heading.

Third, the order is deadline-driven. The U.S. Department of Energy (DOE) must inventory computing resources within 90 days, identify initial data and model assets within 120 days, assess robotic laboratories and production facilities within 240 days, and demonstrate an initial operating capability for at least one challenge within 270 days. For executives, this is a reminder that the federal AI strategy is not just conceptual; there is a concrete implementation timeline that will influence markets and expectations in the near term and it is moving quickly.

The American Science and Security Platform

To execute this vision, the order directs DOE to establish and operate the American Science and Security Platform. This platform is the technical backbone of the Genesis Mission and for businesses, it is effectively the government's AI "engine" for strategic sectors.

The platform must integrate high-performance computing resources (DOE national laboratory supercomputers and secure cloud environments); AI modeling and analysis frameworks (including AI agents that can explore design spaces, evaluate experimental outcomes, and automate research workflows); computational tools (predictive and simulation models and design-optimization tools); and domain-

specific foundation models for the targeted scientific fields. It must also provide secure access to proprietary, federally curated, open, and synthetic datasets, governed under classification, privacy, intellectual property, and federal data-management standards.

In addition, the platform is expected to connect to physical facilities such as robotic laboratories and AI-augmented production environments capable of AI-directed experimentation and manufacturing. Security and resilience are central. DOE is instructed to operate the platform consistent with national security and competitiveness needs, including supply-chain integrity and adherence to federal cybersecurity standards.

For companies, especially those in energy, advanced manufacturing, life sciences, semiconductors, and related supply chains, this is the environment their largest customer – the U.S. government – is building for itself. It will help influence what "good" looks like in terms of data practices, model development, security expectations, and vendor selection.

Why Business Leaders Should Care

Organizations that are not federal agencies will not see an immediate change in their day-to-day compliance obligations from this Executive Order. It functions primarily as an internal directive to federal agencies. But for business leaders, it has several important implications.

First, it is a strategic signal. If your company operates in or around energy, critical materials, biotechnology, advanced manufacturing, quantum technologies, or semiconductors, you should assume that AI capabilities in your space are being treated as matters of national power, not just commercial innovation. That reality will increasingly affect access to capital, export controls, government contracting, and reputational expectations.

Second, it sets up a framework for expanded public-private collaboration. The Genesis Mission anticipates cooperative research and development agreements, user-facility partnerships, and programs that place fellows, interns, and apprentices in national laboratories and other federal research facilities. For businesses that want to participate, that means negotiating detailed terms around data use, model

sharing, intellectual property, classification, export control, and cybersecurity – and living with them over time. This will require a level of AI and data governance that is planned, meaningful, and effective so that it can withstand scrutiny.

Third, it raises expectations for AI governance across the federal supply chain. For companies already in, or aspiring to enter, the federal government supply chain, it will be increasingly prudent to build AI strategy and governance programs that align with the NIST AI Risk Management Framework (AI RMF) as the primary reference for federal risk expectations, and ISO/IEC 42001 as a more practical, certifiable management system that is more actionable as well as recognized internationally. NIST AI RMF provides the risk-based structure federal agencies are likely to use; ISO 42001 offers detailed control and process requirements that business partners, auditors, and regulators around the globe will understand. Together, they give business leaders a concrete roadmap for building AI governance that satisfies both government customers and global markets.

Finally, even outside of regulated sectors, there is a norm-setting effect. When the U.S. government treats AI as strategic infrastructure and builds its own hardened AI environment, large enterprises, and critical-infrastructure operators will face pressure from investors, customers, and insurers to demonstrate that their AI practices are comparably thoughtful and controlled.

State AI Laws, Preemption, and the Reality of Governance

With state-level AI and algorithmic accountability laws proliferating, business leaders also want to know whether the Genesis Mission AI Executive Order changes that landscape. On its face, it does not.

The order contains no preemption clause and does not purport to displace state AI, privacy, consumer protection, or anti-discrimination statutes. Its focus is on federal infrastructure and coordination. Other initiatives in the future may seek to challenge specific state AI laws on constitutional or statutory grounds, but those efforts would be separate and will involve their own legal and political battles.

From a practical business perspective, the more important point is that many state AI laws are, in substance, codifications of sound AI governance practice. Across jurisdictions, common themes appear. In practice, regulators, standards bodies, and

leading organizations expect companies to:

1. **Have a clear AI strategy and governance program** that aligns AI initiatives with business objectives, risk appetite, and legal obligations.
2. **Establish an AI governance committee or similar oversight body** that brings together legal, compliance, security, privacy, and business leadership to oversee AI risk**.**
3. **Know which AI systems you are using and where they sit in your operations**, including an inventory of models, tools, and use cases.
4. **Understand the data those systems consume and the decisions or outputs they produce**, including data lineage, quality, and the populations affected.
5. **Adopt core AI policies and procedures** that define acceptable uses, approval and change-management processes, documentation and testing standards, and escalation paths when issues arise.
6. **Assess and document risks, particularly for high-impact or high-stakes uses**, such as those affecting individuals' rights, safety, employment, financial opportunities, or access to essential services.
7. **Manage AI-related third-party and supply-chain risk**, including vendors, models, data sources, and APIs you do not control, through due diligence, contractual protections, and ongoing monitoring.
8. **Implement appropriate human oversight and escalation paths**, ensuring that humans can understand, challenge, and override AI-driven decisions where necessary.
9. **Provide training to personnel** involved in developing, deploying, or relying on AI systems so they understand both the capabilities and limitations of these tools.
10. **Continuously monitor, test, and adjust AI systems over time**, including performance, drift, bias, security, and alignment with policy and legal requirements.

These expectations align closely with frameworks like NIST AI RMF and ISO/IEC 42001, and with what sophisticated organizations are already doing to manage AI risk. The legal source of the obligation may shift but the principles remain the same. The substance of what responsible AI governance looks like is less likely to change dramatically.

For boards, general counsel, CISOs, and other business leaders, the practical takeaway is straightforward: the Genesis Mission Executive Order confirms that AI has entered the category of strategic importance in a new cold war environment. That speaks directly to the power and importance of AI. In that setting, waiting for clarity on the laws before building a mature AI governance program is not a defensible strategy. Organizations – especially those in the federal supply chain – that align their AI strategy and governance with NIST AI RMF and ISO/IEC 42001, and that internalize the core principles reflected in state, federal, and international laws and regulations, will be better positioned to adapt to future rules, reduce litigation and enforcement risk, and compete effectively in the AI-driven economy this order anticipates.

This blog was drafted by Shawn Tuma, an *attorney in the Spencer Fane Plano, Texas office and the leader of the firm's Cyber | Data | Artificial Intelligence | Emerging Technology team. For more information, visit www.spencerfane.com.*

Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.