ML STRATEGIES

AI: The Washington Report — July 2026 Edition

July 08, 2026 | Article | By **Alexander Hecht**, **Erek L. Barron**, Nicole Y. Teo

VIEWPOINT TOPICS

- AI: The Washington Report

Main Points

- **The White House is moving toward structured federal engagement with frontier AI developers.** On June 2, President Trump released Executive Order 14409, which establishes a voluntary framework for pre-release government review of advanced AI models, with implications for organizations operating or relying on critical infrastructure systems.
- **AI policy and requirements in national security are accelerating.** Also in June, the White House released a National Security Presidential Memorandum that directs the national security enterprise to rapidly adopt AI across intelligence and warfighting domains, including provisions on vendor control and contract accountability that may affect defense contractors, technology companies, and research institutions.
- **The US House introduces comprehensive federal AI governance framework.** The Great American AI Act bipartisan discussion draft legislation proposes transparency mandates, third-party audits, and a three-year preemption of state AI development laws.
- **The US House Science Committee marks up 10 bipartisan AI bills.** Ten bipartisan AI bills advanced in a single markup session in the House Science, Space, and Technology Committee, spanning research access, cybersecurity, workforce development, transparency, and data center energy standards, signaling that Congress is laying technical and institutional groundwork for more substantive AI oversight ahead.
- **AI content labeling requirements are gaining bipartisan support.** The AI Labeling Act of 2026, a bipartisan bill introduced in the Senate, would require disclosure of AI-generated content across major platforms, with potential implications for organizations producing AI-generated content at scale.
- **State-level AI governance continues to expand.** Illinois's passage of S.B. 315, the Artificial Intelligence Safety Measures Act, marks the first state requirement for annual independent third-party audits of frontier AI models, adding to a growing patchwork of state obligations that organizations across industries must navigate.

White House Executive Actions

1. White House Establishes Voluntary Pre-Release Framework for Frontier AI Models

On June 2, 2026, President Trump signed **Executive Order 14409**, "Promoting Advanced Artificial Intelligence Innovation and Security," directing federal agencies to establish a framework for the secure deployment of frontier AI models. The order focuses on three areas:

- upgrading the cyber defenses of government information systems,
- establishing a voluntary framework for developers of frontier AI models to engage with the government prior to deployment, and
- directing enforcement resources toward criminal misuse of AI.

The order imposes 30-day deadlines on multiple agencies to prioritize cyber defense of national security systems and civilian federal government systems. It directs the Secretary of Homeland Security to release Binding Operational Directives to expedite cybersecurity improvements and expand access to AI-enabled defensive tools for critical infrastructure operators, including rural hospitals, community banks, and local utilities.

Central to the EO is a voluntary framework under which AI developers may provide government agencies with pre-release access to "covered frontier models" or highly advanced AI systems meeting classified cybersecurity capability thresholds, for up to 30 days before broader release. The government will develop classified benchmarks to determine which models qualify. The order expressly states it does not authorize the creation of any mandatory licensing, preclearance, or permitting requirement for AI model development or distribution.

The order also directs the formation of an AI cybersecurity clearinghouse, coordinated by the Treasury Department, to identify, validate, and remediate software vulnerabilities, and instructs the US Attorney

General to prioritize enforcement of federal criminal laws against AI-enabled cybercrimes.

Why it matters: Organizations operating critical infrastructure, including in health care, financial services, energy, and other sectors, should monitor the forthcoming cybersecurity directives and the details of the voluntary frontier model engagement framework, which could shape compliance expectations and access to federal cybersecurity tools. The EO's definition of "covered frontier models" through classified benchmarks may also interact with state-level frontier model laws in California, New York, and Illinois, which use computational power thresholds to define covered models.

2. National Security Presidential Memorandum (NSPM-11) Accelerates Military AI Adoption and Tightens Vendor Accountability

On June 5, 2026, the White House issued a National Security Presidential Memorandum, **NSPM-11**, directing the national security enterprise to responsibly accelerate AI adoption across intelligence and warfighting domains. The memorandum rescinds and replaces the Biden administration's NSM-25, which the current administration characterized as imposing undue bureaucracy and fostering "dangerous single-vendor dependencies."

NSPM-11 is organized around four pillars: adoption, adaptation, assurance, and accountability. It directs the rapid onboarding of advanced AI models from multiple vendors, the buildout of high-security computing facilities to run future AI systems at scale, and the establishment of an AI National Security Strategic Reserve of top nongovernmental experts.

The memorandum directs the Secretary of Defense to issue an updated directive on autonomy in weapon systems, to be reviewed annually to keep pace with advancing AI capabilities. It also requires that no commercial entity or adversary possess the capability to prevent use of, disable, degrade, or materially modify an AI system that warfighters depend on without prior government approval.

Notably, NSPM-11 directs agency heads to terminate contracts, for default or convenience, with companies that have "repeatedly demonstrated a pattern of conduct" inconsistent with the administration's policies. It also bars the national security enterprise from developing or using AI to censor free speech, embed ideological bias, or conduct unauthorized or unlawful surveillance.

Why it matters: Defense contractors, research institutions with national security affiliations, and organizations involved in dual-use AI applications should assess how NSPM-11's vendor accountability provisions, contract requirements, and talent pipeline initiatives may affect their operations.

Congressional Activity

3. House Proposes Comprehensive Federal AI Framework with Three-Year State Preemption

On June 4, 2026, Reps. Jay Obernolte (R-CA) and Lori Trahan (D-MA) **released** a 269-page bipartisan discussion draft of the Great American Artificial Intelligence Act (GAAIA), the first comprehensive federal AI governance framework proposed in Congress. The bill is organized around four titles:

- Frontier AI Governance
- Workforce
- Cybersecurity
- Research, Development, and International Cooperation

Key provisions include:

- **Transparency and auditing:** Frontier AI model developers would be required to disclose information about their models and obtain third-party audits through designated Independent Verification Organizations (IVOs).
- **Federal preemption:** A three-year preemption of state laws "specifically regulating the development of" any AI model, where "development" is broadly defined as acts performed by a developer prior to deployment. The preemption does not extend to post-deployment activities or state laws of general applicability, leaving many existing privacy, consumer protection, and health care regulations intact.
- **Workforce provisions:** Enhanced federal data collection on AI's labor market impact and additional transparency when AI is a substantial factor in qualifying mass layoffs.
- **Cybersecurity:** Extension of the Cybersecurity Information Sharing Act of 2015 through fiscal year 2035.

The bill is primarily aimed at the largest AI developers, those with over $500 million in annual revenue, building cutting-edge models, rather than typical deployers. Narrowing the scope to large AI developers is in alignment with how other states like Colorado and California have approached AI governance. The bill

has not yet been formally introduced, and its sponsors are seeking feedback from stakeholders.

Why it matters: Organizations developing or deploying AI should monitor the GAAIA's evolution closely. If ultimately enacted, the discussion draft's transparency requirements, audit mechanisms, workforce provisions, and preemption framework could significantly affect AI development and deployment practices across industries, particularly for companies navigating the current patchwork of state AI laws.

4. House Science, Space, and Technology Committee Advances 10 AI Bills Spanning Research, Security, Workforce, and Transparency

On June 25, 2026, the House Science, Space, and Technology Committee marked up and favorably reported **10 AI-related bills** in a session, signaling a legislative push on AI research and development policy in Congress. All 10 bills passed with strong bipartisan support, most unanimously. The bills span AI research infrastructure, security, workforce development, transparency, and data governance:

- **H.R. 2385, CREATE AI Act** (29-0): Establishes the National Artificial Intelligence Research Resource (NAIRR) to expand access to computing power and datasets for AI research, formally codifying a resource initially established during the Biden administration and housed within the National Science Foundation.
- **H.R. 9363, AI Security and Innovation Act** (29-0): Strengthens the federal approach to securing AI systems, improves coordination across government and industry, and promotes the development of secure, resilient, and trustworthy AI technologies.
- **H.R. 9341, AI-Ready Federal Data Guidelines Act** (29-0): Directs NIST to develop voluntary guidelines to help federal agencies prepare datasets for use in training AI models, aiming to improve the quality and usability of federal data for AI innovation.
- **H.R. 6461, READ AI Models Act** (35-0): Directs NIST to establish a pilot program to develop voluntary resources for documenting AI models, including standardized templates and technical guidance to improve transparency around model development and deployment.
- **H.R. 9333, AI Flaw Reporting and Security Enhancement Act** (35-0): Directs NIST, in consultation with CISA, to establish a voluntary program for reporting and tracking AI vulnerabilities, failures, and other flaws, including a national database.
- **H.R. 8893, Protecting Consumers from Deceptive AI Act** (35-0): Directs NIST to support research, testing, and standards development for technologies that can detect, authenticate, and disclose the origin of digital content, including AI-generated content.
- **H.R. 9334, Workforce for AI Trust Act** (35-0): Directs NIST to expand its AI workforce activities and develop a national framework identifying the tasks, knowledge, and skills needed for AI-related work.
- **H.R. 5351, NSF AI Education Act** (33-0): Expands AI education and workforce training programs at the National Science Foundation, supporting scholarships, fellowships, and professional development.
- **H.R. 5584, LIFT AI Act** (34-1): Authorizes the National Science Foundation (NSF) to support programs promoting AI literacy for K-12 students and educators.
- **H.R. 9372, Data Infrastructure Energy Measurement and Standards Act** (34-1): Directs NIST, in consultation with DOE, to improve how data center energy and water use are measured, reported, and analyzed.

The 10 bills passed in the House Committee reflect a comprehensive, infrastructure-first approach to AI governance. They are primarily focused on investing in the technical, research, and workforce capabilities necessary to further AI development and governance. Notably, many of the bills assign responsibilities to NIST and the NSF, signaling that Congress views these agencies as central to developing the technical standards, research infrastructure, and guidance that will underpin future federal AI policy.

Why it matters: The scope of the markup spans access to AI research resources, model transparency, AI security, and data center energy measurement, suggesting Congress is focused on building the foundation for a broader federal AI governance framework. While these bills do not impose prescriptive regulatory requirements, they could shape future federal standards and best practices, making them worth monitoring as organizations prepare for evolving AI governance and compliance expectations.

5. Bipartisan Senate Bill Would Mandate Disclosure of AI-Generated Content

On June 25, 2026, Sens. Brian Schatz (D-HI), John Curtis (R-UT), and Mark Warner (D-VA) **introduced** the AI Labeling Act of 2026, bipartisan legislation requiring providers of generative AI systems to attach visible and machine-readable disclosures to AI-generated audio, video, and image content.

Under this bill, large online platforms with at least 10 million monthly US users or more than $1.5 billion in annual revenue would be required to flag AI-generated content and barred from stripping out disclosures. The FTC would enforce the requirements, and NIST would convene a working group to set technical standards for labeling and detecting AI content.

The bill is endorsed by SAG-AFTRA, the Songwriters Guild of America, the Authors Guild, and other creative industry organizations.

Why it matters: Organizations using generative AI to produce consumer-facing communications, marketing materials, educational content, or other public-facing outputs should assess whether their use cases would trigger disclosure obligations under this or similar legislation. The bill's reliance on NIST for technical standards connects it to the GAAIA's proposed codification of CAISI within the Commerce Department, which would also develop voluntary AI guidelines and standards. Additionally, the December 2025 Executive Order on ensuring a national AI policy framework emphasized federal interest in preempting inconsistent state-level content labeling requirements, raising questions about how this bill would interact with existing or proposed state AI disclosure laws, **as we've previously covered**.

State-Level Developments

6. Illinois Becomes First State to Require Independent Third-Party Audits of Frontier AI Models

The Illinois General Assembly **passed** the Artificial Intelligence Safety Measures Act (**S.B. 315**), with the House passing the bill unanimously on May 27, 2026 following Senate passage. The bill was sent to Governor Pritzker on June 26, 2026, and the Governor has indicated he will sign it into law, with an effective date of January 1, 2027.

S.B. 315 would be the first state law to require annual independent third-party audits of frontier AI models' safety practices. The bill targets the largest frontier developers, those with over $500 million in annual revenue, developing models above a specified computational power threshold.

Key requirements include:

- Creation and publication of safety frameworks, with annual updates
- Pre-deployment transparency reports
- Reporting of critical safety incidents within 72 hours
- Whistleblower protections
- Filing of disclosure statements with primary contacts and places of business
- Payment of proportional fees to cover administration of the Act

The Illinois Attorney General would have exclusive enforcement authority, with civil penalties of up to $3 million per violation. The bill does not create a private right of action. The legislation is modeled after 2025 laws in California and New York, with Illinois being the first to require third-party audits.

Why it matters: AI developers across industries should evaluate whether their models meet the bill's thresholds and prepare for potential audit and reporting obligations. The growing patchwork of state frontier AI laws, now spanning California, New York, and Illinois, underscores the need for coordinated compliance strategies, particularly as the federal GAAIA proposes a limited preemption of state-level AI development regulations.

We will continue to monitor, analyze, and issue reports on these developments. Please feel free to contact us if you have questions about current practices or how to proceed.

Authors

Alexander Hecht, Executive Vice President & Director of Operations

Alex Hecht is a trusted attorney and policy strategist with over 20 years of experience advising clients across a broad range of industries on how to navigate complex policy environments. His strategic insight and hands-on experience in both legislative and regulatory arenas empower clients to advance their priorities with clarity and confidence in an evolving policy landscape.

Erek L. Barron

Erek L. Barron, a Member at Mintz, is a nationally respected former United States Attorney and seasoned litigator with more than two decades of experience handling complex criminal, civil, and regulatory matters, including leading significant white collar crime, cybercrime, and national security cases.

Nicole Y. Teo

Nicole Y. Teo is a Mintz Senior Project Analyst based in Washington, DC.