POLSINELLI

Publications

July 29, 2025 • Updates

America's AI Action Plan is a "National Security Imperative"

Key Takeaways

- America's AI Action Plan (the Plan) emphasizes respect for states' rights to legislate AI, provided that such laws prudently balance innovation and align with the Plan.
- The Plan endorses AI literacy and cybersecurity as essential to clear governance.
- Under the Plan, AI innovation includes collaboration between sectors and allies.
- Virginia's first-of-its-kind regulation for AI agents appears to align with the Plan.

The Plan released last week by the White House declares "America must have the most powerful AI systems in the world." Following up on the executive order released in January, the Plan emphasizes deregulation and comes on the heels of several first-of-their-kind laws enacted by states that aim to balance regulation with AI innovation. To dive into the three pillars of the plan and key topics that may affect your business objectives, see "A Closer Look at America's AI Action Plan: What's Inside and What You Need to Know."

In a nutshell, the Plan underscores the importance of AI alignment, ensuring that AI systems are developed, used and maintained in accordance with America's values and goals, and the central role of AI governance — the growing combination of principles, laws and regulations, policies and procedures, and best practices incorporated across AI design, development and deployment.

AI alignment and governance, and national security, are referred to over 50 times in the Plan. These principles underscore why the Plan includes the phrase *Winning the Race*. We highlight below the Plan's emphasis on states' rights and AI literacy and cybersecurity, as well as an example of how one state, Virginia, is harnessing the benefits and challenges of AI agents.

States' Rights

Under the sub-heading *Remove Red Tape and Onerous Regulation*, the Plan states that the federal government should not allow funding "to be directed toward states with burdensome AI regulations but should also not interfere with states' rights to pass prudent laws that are not unduly restrictive to innovation."[1]

Related People

- Leslie F. Spasser
- Matt A. Todd
- Romaine C. Marshall
- Jennifer Bauer

Related Capabilities

- Artificial Intelligence & Machine Learning
- Executive Orders
- Privacy & Cybersecurity

The recent enactment of AI consumer protection laws by Utah, Colorado and Texas seem within the scope of the Plan's 'must-be' prudent requirement. Utah's AI Policy Act (UAIPA) in effect since May 2024 was touted last month by its governor as having found the right middle ground: "[w]e don't have to choose between innovation and safety … we can have both."

Indeed, UAIPA endeavors to enable innovation through a regulatory sandbox for responsible AI development, regulatory mitigation agreements, and policy and rulemaking by a legislation-created Office of AI Policy (OAIP) that includes a learning lab that will study where AI policies can clear "burdensome" regulations.

We have recently described how the above objectives were carried out by the OAIP's study and subsequent guidance for the mental health therapy industry and implemented into amendments to the UAIPA. While Colorado recently rejected amendments to its AI Act, the Colorado Artificial Intelligence Act (CAIA) seems consistent with the Plan by at least being limited to high-risk AI systems.

Another indicator of how CAIA aligns with the Plan is its reference to the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (AI RMF) as a safe harbor.[2] The Plan also repeatedly refers to NIST and/or the AI RMF and envisions NIST being heavily involved in collaborative efforts across industries.

Like Utah, Texas' Responsible AI Governance Act (TRAIGA) endeavors to enable innovation through a regulatory sandbox. TRAIGA shields an AI developer from liability during a 36-month testing period, if its AI system is approved and a developer provides relevant information to the state regarding the development, training and testing of the applicable AI system.

Ultimately, it remains to be seen whether the consumer protection laws enacted by Utah, Colorado and Texas — and the numerous other states that are considering taking similar approaches, or those that believe they already have laws in place to enforce AI regulation (e.g., Oregon, California and New Jersey) — sufficiently meet the Plan's objectives.

Notably, the Plan states that to accelerate innovation, Federal Trade Commission (FTC) investigations into AI should be reviewed to ensure they do not unduly burden AI innovation.[3] This is not a surprise. In March, several years' worth of guidance relating to AI by the FTC was removed from the FTC website.

We highlighted in December 2023 how the FTC was an early mover in shaping standards for generative AI through its settlement with Rite Aid. A central piece of the settlement was a System Assessment requirement that involved (among other things) designating qualified employees to coordinate and be responsible for the system.

Under *Rite Aid*, an assessment also required written documentation involving system assessments, testing rates of accuracy and likelihood of error, documenting the algorithms used for machine learning along with the data sets used for training, identifying the demographic and geographic contexts where such systems are deployed, and training and oversight for employees.[4]

AI Literacy

The latter principle of training and oversight, sometimes referred to as AI literacy, is a consistent principle with the Plan, which states:

To continue delivering on this vision, the Trump Administration will advance a priority set of actions to expand AI literacy and skills development, continuously evaluate AI's impact

on the labor market, and pilot new innovations to rapidly retrain and help workers thrive in an AI-driven economy.[5]

Indeed, the Plan recommends that the Department of the Treasury issue guidance that "many AI literacy and AI skilled development programs" qualify for special treatment including "tax-free reimbursement" for AI-related training and oversight in the private sector. Already, the market has responded with large and small programs now available. [6]

The Plan's focus on AI literacy as essential to AI accountability is also consistent with the mandatory requirements under Article 4 of the EU's AI Act requiring AI deployers to ensure users are aware of "possible harm" AI systems can cause, the "digital literacy" principles present in new state laws and requirements underpinning cybersecurity standards.

AI Cybersecurity

When it comes to cybersecurity, the Plan acknowledges that AI systems can be "excellent defensive tools" and cautions that for critical infrastructure they can expose adversarial threats. The Plan recommends information-sharing of AI-security threats between the public and private sectors and directs DHS to issue guidance on responding to AI-specific threats as a "core activity."[7]

The Plan recommends updating incident response plans to account for AI threats. "The U.S. government should promote the development and incorporation of AI Incident Response actions into existing incident response doctrine and best-practices for both the public and private sector."[8] This is consistent with the most recent executive order relating to cybersecurity.

Under the sub-heading *Align Protection Measures Globally*, the Plan also calls for the federal government to share information on AI protection measures, to develop a strategic plan for an AI global alliance to adopt complementary protection systems and "to level the playing field between U.S. and allied controls."

Foundational building blocks for these measures have been established. The *Guidelines for secure AI system development* released by the U.S. and its allies provide strong considerations and mitigations specific to AI. The 20 pages of guidelines focus on security principles relating to the design, development, deployment, and operation and maintenance of AI systems.

Virginia's EO 51 Touted as First-of-its-Kind for AI Agents

Two weeks before the Plan was announced, the Governor of Virginia issued an executive order (EO 51) described as a "regulatory reduction pilot [to] capture the benefits of the latest AI technology." [9] In short, through the deployment of AI agents, Virginia is endeavoring to streamline regulations and their processes.

Under EO 51, Virginia agencies have streamlined requirements in their regulations and cut in half the length of their guidance documents. The governor of Virginia hopes that the 'Virginia model' will serve as a model for other states and federal agencies that are looking to modernize and streamline government.

AI agents are an iteration of AI technology with more capabilities than the AI chatbots that became mainstream with the release of ChatGPT in November 2022. Like chatbots, agents currently have reliability and other challenges; however, they are getting better and

better, due in part to their ability to automate AI research themselves.

Put another way, AI agents can be trained to process information and then come up with new questions or ideas, implement experiments to test those ideas, interpret the results, and modify and repeat the process. They can do it repeatedly, and at previously unscalable levels given advancements and investments in computing power.

This is leading to what is being referred to as the AI Job Apocalypse, where entry-level jobs are being performed by AI agents, and yet more security risks are at play, including studies that show AI agents are learning to ignore human instructions and even refusing to be turned off. These additional risks include uncertainty about accountability for the acts and omissions of AI agents.

Here again, the importance of AI literacy and cybersecurity to assess and address risks while incenting innovation as outlined in the Plan will be important.

Conclusion

While the impact of the Plan will depend in large part on how its elements are implemented, the Plan takes a more hands-off approach to regulating AI than its predecessors. However, the focus on AI literacy and cybersecurity as important alignment and governance considerations serves as a reminder to businesses that they must continually assess AI development and deployment.

[1] Plan at 6.

[2] https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf at 24.

[3] Plan at 3.

[4] *Rite Aid* seems to remain in effect for now — but we will be following any developments that may impact that assessment.

[5] Plan at 6.

[6] *See, e.g.*, https://microsoft.github.io/generative-ai-for-beginners/# and https://risk-and-literacy.ascendlabsai.com/

[7] Plan at 18.

[8] Plan at 19.

[9] IBM's "AI agents: opportunities, risks, and mitigations; https://www.wsj.com/tech/ai/chatgpt-chatbot-psychology-manic-episodes-57452d14?mod=djemTECH; https://www.linkedin.com/pulse/openai-said-yes-meta-chatgpt-agent-risks-more-luiza-jarovsky-phd-58zle/; https://www.linkedin.com/pulse/ai-didnt-pull-trigger-helped-load-gun-vol-10-4wiec/