Akin℠

Lawmakers, White House and Industry Continue the Push for AI Regulation

By **Hans Rickhoff, Ed Pagano, Reggie Babin**, **Alan Hayes, and Taylor Daly**

July 31, 2023

Key Points

- In recent weeks, both policymakers and industry have announced a slew of initiatives to regulate the development and use of artificial intelligence.

- Most recently, the White House announced voluntary commitments that seven leading AI companies are taking to manage the risks of new AI development and use, with a broader executive order and legislative effort underway. Separately, several of the companies have convened an industry forum to advance AI research and develop best practices.

- Both chambers of Congress have also worked in recent weeks to advance their respective versions of must-pass defense legislation with key AI provisions.

- Lawmakers are also prepping their own standalone AI legislation, including Sen. John Thune (R-SD), who plans to introduce an AI certification measure following the August recess.

White House Partners with Industry on AI Commitments and Develops Broader Executive Order; Industry Stands Up AI Forum

On July 21, 2023, the White House **announced** new, **voluntary commitments** made by seven leading artificial intelligence (AI) companies—Amazon, Anthropic, Google, Inflection, Meta, Microsoft and OpenAI—to manage the risks of new AI development and use, based on three overarching principles of safety, security and trust. The companies' commitments include:

- **Safety**: Internal and external security testing of their AI systems, conducted in part by independent experts, as well as information sharing amongst industry and with governments, civil society and academia on managing AI risks.

- **Security**: Investments in cybersecurity and insider threat safeguards, as well as enabling third-party discovery and reporting of vulnerabilities in their AI systems.

- **Trust**: (1) developing comprehensive technical mechanisms to notify users of AI-generated content, such as a watermarking system; (2) publicly reporting their AI systems' capabilities and limitations; (3) prioritizing research on the potential societal risks of AI systems; and (4) deploying advanced AI systems to "help address society's greatest challenges."

Concurrently, the White House indicated that the Biden administration is developing an executive order (EO) and will pursue bipartisan legislation to help the United States (U.S.) lead in AI innovation.

Following the White House announcement, four of the companies—Anthropic, Google, Microsoft and OpenAI—**announced** the creation of the Frontier Model Forum, which aims to, among other things, advance AI safety

research; formulate best practices for the development and deployment of frontier models; and facilitate information-sharing with lawmakers, industry, academics and civil society.

Senate Republican Shops AI Certification Bill; AI Caucus Leaders Introduce Bill to Drive Research

Sen. John Thune, Assistant Republican Leader and a key member of the Senate Commerce Committee, has begun to seek feedback from industry and Members on his draft Artificial Intelligence Innovation and Accountability Act, which he aims to formally introduce after the August recess. The measure would reportedly establish a self-certification system to be regulated and enforced by the U.S. Department of Commerce ("Commerce Department"). The draft legislation would establish the following three categories of AI, each with varying requirements:

1. **Critical High-Impact AI**: Under this category—which is defined to include a system that impacts biometric identification, management of critical infrastructure, criminal justice or fundamental rights—companies would adhere to a five-year testing and certification plan established by the Commerce Department.

2. **High-Impact AI**: Under this category—which is defined to include systems developed to impact housing, employment, credit, education, places of public accommodation, health care or insurance in a manner that poses a significant risk to fundamental rights or safety—companies would be required to self-certify under a separate impact assessment.

3. **Generative AI**: Under this final category, companies would be subject to self-certification requirements only if an application meets the definition of critical high-impact or high-impact. Companies would also be required to notify consumers of a platform's use of generative AI.

The draft legislation also reportedly provides for a number of carve outs, including an exemption for companies with less than 500 employees, or those that collect the personal data of less than one million individuals annually.

Lawmakers, including the leaders of the House and Senate AI caucuses, also continue to explore legislation to improve capacity for AI research, most recently through the introduction of the Creating Resources for Every American To Experiment with Artificial Intelligence Act of 2023 ("CREATE AI Act"; **S. 2714**/**H.R. 5077**). The bill would authorize the establishment of the National Artificial Intelligence Research Resource (NAIRR) to be overseen by the National Science Foundation (NSF). Under the bill, researchers at institutions of higher education, as well as certain small businesses, would be eligible to use the NAIRR for AI research through a merit-based process. NSF would fund the NAIRR through the $1 billion per year authorized to NSF under the National AI Initiative Act (**P.L. 116-283**).

Lawmakers Advance AI Provisions in Must-Pass Defense Bill

Before departing for the August recess, the Senate passed the FY 2024 National Defense Authorization Act (NDAA; **S. 2226**) with bipartisan support via an 86-11 vote, contrasting to the House's near party-line passage of its own NDAA (**H.R. 2670**) earlier this month and teeing up bicameral negotiations over a compromise version of the bill.

The manager's package for the Senate bill included 47 amendments, with 23 proposals from each Democrats and Republicans. In particular, the Senate manager's package **directs** the U.S. Department of Defense (DoD) to establish a Chief Digital and Artifical Intelligence Officer Governing Council, which would meet at least twice each fiscal year, to provide policy oversight to ensure the responsible, coordinated, and ethical employment of data and AI capabilities across DoD missions. The package also **directs** DoD to, within 180 days of enactment, review its current investment into applications of AI and categorize the types of AI investments, and subsequently submit a report of the Department's findings to Congress.

More than 900 **floor amendments** were submitted for consideration. Among these amendments is a **measure** filed by Sen. Michael Bennet (D-CO) directing the White House to set up an AI Task Force comprised of federal agencies' chief privacy and civil liberties officers. Sen. Jerry Moran (R-KS) also filed an **amendment** directing agencies to implement the National Institute of Standards and Technology's (NIST) AI Risk Management Framework.

The previously unveiled Senate NDAA **base text** included a range of AI provisions, including a set of 13 directives which aim to update DoD's broader plans and strategies for AI:

1. **Department-Wide AI Strategy**: Establish and document procedures, including timelines, for the periodic review of the 2018 DoD **Artificial Intelligence Strategy**, or any successor strategy, and evaluate whether any revision is necessary;

2. **Ethical AI Use**: Issue DoD-wide guidance that defines outcomes of near-term and long-term strategies and plans relating to the adoption of AI and its ethical use;

3. **Bias in AI Algorithms**: Issue Department-wide guidance regarding methods to monitor accountability for AI-related activity and mitigate bias in AI algorithms;

4. **Generative AI Plan**: Develop a strategic plan for the development, use and cybersecurity of generative AI;

5. **Workforce Plans**: Assess technical workforce needs across the future years defense plan to support the continued development of AI capabilities, including recruitment and retention policies and programs;

6. **AI Training Materials**: Assess the availability and adequacy of the basic AI training and education curricula available to the civilian workforce and military personnel;

7. **Standardized AI Terminology**: Issue a timeline and guidance for the Chief Digital and Artificial Intelligence Officer and the Secretaries of the military departments to establish a common terminology for AI-related activities;

8. **Integrity of AI Systems**: Implement a plan to protect and secure the integrity, availability and privacy of AI systems and models;

9. **Commercially Available Language Models**: Implement a plan to identify commercially available and relevant large language models;

10. **Adversarial AI**: Develop a plan to defend the systems of the Department against adversarial AI;

11. **IP Protection**: Implement a policy for use by contracting officials to protect the intellectual property of commercial entities that provide their AI algorithms to a Department repository established pursuant to the FY 2022 NDAA;

12. **Control of Data Collection**: Issue guidance and directives for how the Chief Digital and Artificial Intelligence Officer will exercise authority to access, control and maintain data collected, acquired, accessed or utilized by Department components; and

13. **Human Intervention/Oversight**: Clarify guidance on human intervention and oversight in the exercise of AI algorithms for use in the generation of offensive or lethal courses of action for tactical operations.

The House previously passed its version of the NDAA (**H.R. 2670**) on July 14. The House measure also includes a number of AI-focused DoD directives:

• **Responsible Development and Use of AI**: Develop and implement a process (1) to assess whether any AI technology used by the Department is functioning responsibly; (2) to report and remediate any AI technology determined not to be functioning responsibly; and (3) if efforts to remediate such technology are unsuccessful, to discontinue its use until effective remediation is achievable;

- **Centralized Platform for Development and Testing of Autonomy Software**: Conduct a study to assess the feasibility of creating a centralized platform for the development and testing of autonomy software;

- **Optimization of Aerial Refueling in Contested Logistics Environments Through Use of AI**: Commence a pilot program to optimize the logistics of aerial refueling and fuel management through the use of advanced digital technologies and AI; and

- **Framework for Classification of Autonomous Capabilities**: Establish a Department-wide classification framework for autonomous capabilities within 180 days of enactment.

Conclusion

Akin's lobbying & public policy practice continues to closely monitor Congressional, White House and industry activity on AI, and will continue to keep clients apprised of noteworthy advancements, including those that arise as lawmakers ultimately work to reconcile differences between the House and Senate versions of the NDAA for final passage into law later this year. For more information about broader AI policy, regulatory and industry developments, please see our **latest edition of Akin's AI newsletter, Akin Intelligence**.

If you have questions about this client alert, please contact any Akin lawyer or advisor below:

Hans Rickhoff
hrickhoff@akingump.com
+1 202.887.4145

Ed Pagano
epagano@akingump.com
+1 202.887.4255

Reggie Babin
rbabin@akingump.com
+1 202.887.4140

Alan Hayes
amhayes@akingump.com
+1 202.887.4272

Taylor Daly
tdaly@akingump.com
+1 202.416.5541