OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

USA: Senate AI bill and its implications for the private sector

In this Insight article, Michael Rubin and Robert Brown, from Latham & Watkins LLP, explore the contours of the U.S. Senate's recently proposed bipartisan legislation, the Artificial Intelligence Research, Innovation, and Accountability Act of 2023 (AIRIA).

As governments around the globe grapple with how best to regulate the development and use of artificial intelligence (AI) technologies, the US has forcefully entered the fray. On October 30, 2023, President Biden issued a sweeping Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (the Executive Order) calling on all corners of the Federal Government to embrace, research, and regulate AI in the US, structured around eight fundamental guiding principles. A mere two weeks later, a bipartisan group of Senators answered the call by introducing AIRIA.

AIRIA shares much of the Executive Order's core fiber, in particular, its confidence in the inevitable ubiquity of AI and its urgent appeal for risk-based accountability. If enacted, AIRIA would stand as the legislative centerpiece of a national governance framework for the safe, secure, and trustworthy development and use of AI, with considerable implications for organizations that fall within its scope.

Research and innovation

AIRIA comprises two parts. Title I champions AI research and innovation, primarily by amending existing federal law to better account for AI, and directing certain federal agencies to undertake AI-related research. While Title I does not directly regulate the private sector, it will likely play a significant role in formalizing the norms of AI engagement for private sector participants.

Most notably, Title I requires the Director of the National Institute of Standards and Technology (NIST) to explore the development of authenticity and provenance standards for content generated by human authors and AI systems and to carry out a 10-year pilot program to assess the feasibility of using available technologies and creating open standards to achieve this objective. The focus on content authentication and provenance elevates the principle of trust as a governmental priority, echoing the Executive Order's call for the establishment of 'standards and best practices for detecting AI-generated content and authenticating official content.'

Title I also expands the National Institute of Standards and Technology Act's (NIST Act) standards for AI to enable the development of best practices for detecting outputs generated by AI systems and standards for the detection of emergent and anomalous behavior in AI-generated media. It further embeds the concept of AI into federal law by modifying the Open Government Data Act to incorporate 'data models' into the definition of 'public data asset' and separately define 'artificial intelligence system,' signaling a commitment on the part of the Federal Government to transparency in the deployment of AI systems.

Finally, Title I directs the Comptroller General to study barriers to the use of AI systems to improve the functionality of the Federal Government and identify best practices for the Federal Government's adoption and use of AI systems.

Accountability

In Title II, AIRIA defines the parameters for a risk-based AI governance framework and mandates tangible accountability measures, such as transparency reports, risk assessments, and certifications. The primary targets of Title II are deployers of high-impact AI systems (HIAIS) and critical-impact AI systems (CIAIS).

Title II defines HIAIS as an AI system specifically developed with the intended purpose of making decisions that have a legal or similarly significant effect regarding individual access to housing, employment, credit, education, healthcare, or insurance, in a manner that poses a significant risk to constitutional rights or safety. This formulation tracks with existing legal definitions, including under recently enacted state comprehensive privacy laws that grant consumers a right to opt out of the processing of their personal data for such purposes. Title II requires deployers of HIAIS to submit annual transparency reports describing their design and safety plans for the AI systems, and amends the NIST Act to establish a process

for the Director of NIST to make recommendations to various federal agencies regarding the further regulation of the deployment of HIAIS.

CIAIS, on the other hand, is defined as an AI system used or intended to be used for making decisions that have a legal or similarly significant effect on:

- the collection of biometric data without consent;
- the management and operation of critical and space-based infrastructure; or
- criminal justice, in each case, in a manner that poses a significant risk to constitutional rights or safety.

Deployers of CIAIS must complete a risk management assessment at least 30 days prior to making a CIAIS publicly available, submit to the Commerce Secretary a report outlining the assessment no more than 90 days after its completion, and update the assessment on a biennial basis.

Relatedly, the Commerce Secretary must convene an AI Certification Advisory Committee to provide advice and recommendations on testing, evaluation, validation, and verification (TEVV) standards, and the certification of CIAIS. Title II also charges the Commerce Secretary with producing a three-year implementation plan for the certification of CIAIS, to be updated periodically and ultimately submitted to the Advisory Committee and to Congress. Only after such submission is the Commerce Secretary required to issue TEVV standards for CIAIS, to be reviewed by the Advisory Committee prior to publication. Deployers of CIAIS must thereafter self-certify to the Commerce Secretary their compliance with applicable TEVV standards.

Key takeaways for the private sector

Despite the comprehensive nature of the bill, AIRIA retains a generally tight focus, careful not to unnecessarily burden businesses, and resolved to encourage rather than stifle AI-related innovation. At the same time, the obligations that the bill imposes on in-scope businesses are consequential, and it sets the stage for muscular enforcement and a long-term expansion of regulatory oversight. Accordingly, the takeaways for the private sector are a mixed bag, including both encouraging silver linings, but also some warning signs.

First, AIRIA centers on AI systems with the highest potential for harmful outcomes rather than seeking to broadly regulate AI use. As a result, a substantial swath of the private sector

will not bear the direct and immediate brunt of the bill. This risk-based approach echoes both the Executive Order as well as landmark efforts to regulate AI in other jurisdictions, including the EU, Brazil, and Canada. The nascent EU Artificial Intelligence Act (the EU AI Act), for example, classifies AI systems into four risk-based tiers, each of which is subject to different rules of the road. In a similar vein, AIRIA classifies AI systems as HIAIS and CIAIS, constructing each term around categories of AI use that are commonly understood to pose a heightened risk to the rights and safety of individuals.

Second, AIRIA defines several key terms in such a way as to further narrow its application. For example, the bill defines 'significant risk' as a combination of severe, high-intensity, high-probability, and long-duration risk of harm to individuals, and 'significant risk' is, in turn, a critical element of the definitions of both HIAIS and CIAIS. Consequently, AIRIA sets a relatively high bar for AI systems to qualify as HIAIS or CIAIS - only businesses that deploy AI systems for the discrete purposes listed in the definitions of HIAIS or CIAIS and in a manner that poses a significant risk of harm (i.e., severe, high-intensity, etc.) will be directly subject to the bill's central accountability provisions.

AIRIA separately prohibits businesses from operating a covered internet platform (essentially, any website, internet application, or online platform) that uses generative AI without first providing notice of such use to users. But the term 'covered internet platform' expressly precludes platforms owned or operated by businesses that have no more than 500 employees, averaged less than $50 million in annual gross receipts over the most recent three-year period, and collect or process the personal data of less than one million individuals annually. A business that falls below each of these thresholds is not an operator of a covered internet platform and is therefore not required to notify users regarding the use of generative AI.

Third, AIRIA adopts a generally permissive posture. Unlike the proposed bills in the EU and Brazil, for example, AIRIA does not outright prohibit any particular use of AI systems (except in the event that the operator of a covered internet platform fails to provide the requisite notice of generative AI use to users). Rather, it establishes an accountability-based governance framework designed to allow the deployment of AI systems only after they have proven to be safe, reliable, and effective. It also seeks to lessen the compliance burden on in-scope businesses by directing the Commerce Secretary to ensure that the requirements of the bill are not unnecessarily burdensome or duplicative of other agency requirements regarding the non-federal use of HIAIS.

Furthermore, while the bill requires deployers of CIAIS to submit a report outlining their risk management assessment to the Commerce Secretary, it specifically forbids the Commerce Secretary from prohibiting CIAIS deployment while it reviews the report. Finally, AIRIA adopts business-friendly rules of construction in three different sections that offer specific protection for confidential or privileged information, including algorithms, trade secrets, and intellectual property.

Fourth, AIRIA lays the groundwork for meaningful enforcement by the Department of Commerce. The Commerce Secretary may impose civil penalties on deployers of HIAIS or CIAIS who fail to comply with their obligations of up to the greater of $300,000 or the amount that is twice the value of the transaction that forms the basis of the relevant violation. The Commerce Secretary can also prohibit the deployment of AI systems if the violations are intentional and may refer violations to the Attorney General to bring a civil action to enjoin certain violations or collect a civil penalty. Notably, these consequences may result not only from violations of the specific obligations in AIRIA but also from any regulation or order issued thereunder. Helpfully, though, certain violations may be cured within 15 days of notice of the violation without enforcement.

Finally, channeling the Executive Order, AIRIA ensures that the rules and guardrails for the permissible use and development of AI in the US will remain dynamic and may increase in rigor over time. Where the Executive Order calls upon NIST to develop certain guidelines and best practices for AI deployment, including rigorous standards for extensive red-team safety testing, AIRIA goes further by amending the very statute undergirding NIST to enable further administrative supervision. Specifically, the bill modifies the NIST Act to incorporate the definition of HIAIS and to instruct the Director of NIST to develop additional sector-specific recommendations for federal agencies to conduct oversight of HIAIS, including by issuing regulations, standards, or guidelines. In short, the general transparency and accountability requirements for deployers of HIAIS and CIAIS found in AIRIA constitute a floor, not a ceiling.

While AIRIA still faces a long road to becoming law, it marks a significant step forward in governmental efforts to regulate the safe, secure, and trustworthy development and use of AI at the federal level in the US. It also provides the clearest view so far into how lawmakers are thinking about AI and the shape a national AI governance framework may ultimately take. Private businesses should take AIRIA into account when assessing the AI legal landscape for insights into where the chips will ultimately fall.

Michael Rubin Partner
michael.rubin@lw.com
Robert Brown Counsel
robert.brown@lw.com
Latham & Watkins LLP, California and Texas