MINTZ

Commerce Department Launches Cross-Sector Consortium on AI Safety — AI: The Washington Report

February 16, 2024 | Article | By **Bruce D. Sokler**, **Alexander Hecht**, **Christian Tamotsu Fjeld**, Raj Gambhir

VIEWPOINT TOPICS

- Artificial Intelligence
- Antitrust
- ML Strategies

RELATED PRACTICES

- Antitrust
- Lobbying and Public Policy

RELATED INDUSTRIES

1. The Department of Commerce has launched the **US AI Safety Institute Consortium** (AISIC), a multistakeholder body tasked with developing AI safety standards and practices.
2. The AISIC is currently composed of **over 200 members** representing industry, academia, labor, and civil society.
3. The consortium may play an important role in implementing key provisions of President Joe Biden's executive order on AI, including the development of guidelines on red-team testing**[1]** for AI and the creation of a companion resource to the **AI Risk Management Framework**.

Introduction: "First-Ever Consortium Dedicated to AI Safety" Launches

On February 8, 2024, the Department of Commerce announced the creation of the **US AI Safety Institute Consortium** (AISIC), a multistakeholder body housed within the National Institute of Standards and Technology (NIST). The purpose of the AISIC is to facilitate the development and adoption of AI safety standards and practices.

The AISIC has brought together over 200 organizations from industry, labor, academia, and civil society, with more members likely to join in the coming months.

Biden AI Executive Order Tasks Commerce Department with AI Safety Efforts

On October 30, 2023, President Joe Biden signed a wide-ranging **executive order on AI** ("AI EO"). This executive order has mobilized agencies across the federal bureaucracy to implement policies, convene consortiums, and issue reports on AI. Among other provisions, the AI EO directs the Department of Commerce (DOC) to establish "guidelines and best practices, with the aim of promoting consensus…[and] for developing and deploying safe, secure, and trustworthy AI systems."

Responding to this mandate, the DOC established the **US Artificial Intelligence Safety Institute** (AISI) in November 2023. The role of the AISI is to "lead the U.S. government's efforts on AI safety and trust, particularly for evaluating the most advanced AI models." Concretely, the AISI is tasked with developing AI safety guidelines and standards and liaising with the AI safety bodies of partner nations.

The AISI is also responsible for convening multistakeholder fora on AI safety. It is in pursuance of this responsibility that the DOC has convened the AISIC.

The Responsibilities of the AISIC

"The U.S. government has a significant role to play in setting the standards and developing the tools we need to mitigate the risks and harness the immense potential of artificial intelligence," said DOC Secretary Gina Raimondo in a **statement** announcing the launch of the AISIC. "President Biden directed us to pull every lever to accomplish two key goals: set safety standards and protect our innovation ecosystem. That's precisely what the U.S. AI Safety Institute Consortium is set up to help us do."

To achieve the objectives set out by the AI EO, the AISIC has convened leading AI developers, research institutions, and civil society groups. At launch, the AISIC has over 200 members, and that number will

likely grow in the coming months.

According to NIST, members of the AISIC will engage in the following objectives:

1. Guide the evolution of industry standards on the development and deployment of safe, secure, and trustworthy AI.
2. Develop methods for evaluating AI capabilities, especially those that are potentially harmful.
3. Encourage secure development practices for generative AI.
4. Ensure the availability of testing environments for AI tools.
5. Develop guidance and practices for red-team testing and privacy-preserving machine learning.
6. Create guidance and tools for digital content authentication.
7. Encourage the development of AI-related workforce skills.
8. Conduct research on human-AI system interactions and other social implications of AI.
9. Facilitate understanding among actors operating across the AI ecosystem.

To join the AISIC, **organizations were instructed** to submit a letter of intent via an online webform. If selected for participation, applicants were asked to sign a Cooperative Research and Development Agreement (CRADA)**[2]** with NIST. Entities that could not participate in a CRADA were, in some cases, given the option to "participate in the Consortium pursuant to separate non-CRADA agreement."

While the initial deadline to submit a letter of intent has passed, NIST has provided that there "may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter of interest after the selection process." Inquiries regarding AISIC membership may be directed to **this email address**.

Conclusion: The AISIC as a Key Implementer of the AI EO?

While at the time of writing NIST has not announced concrete initiatives that the AISIC will undertake, it is likely that the body will come to play an important role in implementing key provisions of Biden's AI EO. As discussed earlier, NIST created the AISI and the AISIC in response to the AI EO's requirement that DOC establish "guidelines and best practices…for developing and deploying safe, secure, and trustworthy AI systems." Under this general heading, the AI EO lists specific resources and frameworks that the DOC must establish, including:

- A "companion resource" to the NIST **AI Risk Management Framework**.
- Guidelines for the deployment of red-team testing for AI systems.
- Policies to support the development and deployment of privacy-enhancing technologies (PETs) and testbeds for the development of safe AI.
- Guidelines for the assessment of **dual-use foundation models**.
- A "companion resource" to the NIST **Secure Software Development Framework** that reflects recent advances in AI.

It is premature to assert that either the AISI or the AISIC will exclusively carry out these goals, as other bodies within the DOC (such as the National AI Research Resource) may also contribute to the satisfaction of these requirements. That being said, given the correspondence between these mandates and the goals of the AISIC, along with the multistakeholder and multisectoral structure of the consortium, it is likely that the AISIC will play a significant role in carrying out these tasks.

We will continue to provide updates on the AISIC and related DOC AI initiatives. Please feel free to contact us if you have questions as to current practices or how to proceed.

Endnotes

[1] As explained in our July 2023 newsletter on Biden's voluntary framework on AI, "red-teaming" is "a strategy whereby an entity designates a team to emulate the behavior of an adversary attempting to break or exploit the entity's technological systems. As the red team discovers vulnerabilities, the entity patches them, making their technological systems resilient to actual adversaries."

[2] See "CRADAs - Cooperative Research & Development Agreements" for an explanation of CRADAs. **https://www.doi.gov/techtransfer/crada**.

Authors

Bruce D. Sokler, Member / Co-chair, Antitrust Practice

Bruce D. Sokler is a Mintz antitrust attorney. His antitrust experience includes litigation, class actions, government merger reviews and investigations, and cartel-related issues. Bruce focuses on the health care, communications, and retail industries, from start-ups to Fortune 100 companies.

Alexander Hecht, ML Strategies - Executive Vice President & Director of Operations

Alexander Hecht is Executive Vice President & Director of Operations of ML Strategies, Washington, DC. He's an attorney with over a decade of senior-level experience in Congress and trade associations. Alex helps clients with regulatory and legislative issues, including health care and technology.

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Raj Gambhir

Raj Gambhir is a Project Analyst in the firm's Washington DC office.

More Viewpoints

Senators Propose Clarification of Antitrust Law to Expressly Cover Algorithmic Collusion — *AI: The Washington Report*

February 8, 2024 | Article | By Bruce Sokler, Alexander Hecht, Christian Tamotsu Fjeld, Raj Gambhir

Read more