THOUGHT LEADERSHIP

PUBLISHED: FEBRUARY 12, 2024

NIST Introduces the Leaders of the Artificial Intelligence Safety Institute, and Announces the Institute's AI Consortium

Service

Artificial Intelligence

Professional

ERIK DULLEA
DENVER:
303.749.7270
ERIK.DULLEA@
HUSCHBLACKWELL.COM

NIST DEBUTS THE INITIAL STEPS TO TACKLE THE CHALLENGES OF AI

On February 7, 2024, Secretary of Commerce Gina Raimondo introduced Elizabeth Kelly and Elham Tabassi as the inaugural director and chief technology officer (CTO) of the U.S. Artificial Intelligence Safety Institute (USAISI).

The USAISI will operate under the National Institute of Standards and Technology (NIST) and is directed to develop guidelines, evaluate models, and pursue research related to the tasks assigned to NIST by President Joseph Biden's Executive Order, described in our prior analysis in November 2023.

Introduction of the USAISI Consortium and inaugural members

The day after the USAISI leadership announcement, Secretary Raimondo announced the creation of a consortium intended to bring together artificial intelligence (AI) creators and users, academic institutions, government and industry researchers, and civil society organizations to support the development and deployment of safe and trustworthy AI. The USAISI Consortium, tagged with the acronym AISIC, includes over 200 members from academia, advocacy organizations, private industry, and the public sector.

This initial cadre of members was selected from the applicant window that opened on November 2, 2023, when the USAISI was originally announced. For interested stakeholders who missed the original application window, the

Consortium's FAQ webpage confirms there will be additional announcements inviting organizations to join the AISIC in the future, and in most cases members are required to enter into a consortium Cooperative Research and Development Agreement (CRADA) with NIST.

Objectives for the AISIC

As the director, Kelly will be responsible for coordinating USAISI activities with other AI policy and technical initiatives across the Commerce Department, NIST, and the federal government. In her role as CTO, Tabassi will be responsible for leading USAISI's key technical programs to develop and deploy AI that is "safe, security and trustworthy." Readers will recognize those goals as coming directly from the Executive Order.

According to NIST, AISIC will initially focus on enabling the development and deployment of safe and trustworthy AI systems through the operationalization of NIST's AI Risk Management Framework (AI RMF) and addressing the challenges identified under NIST's AI RMF roadmap. Like its Cybersecurity Framework, adoption of the NIST AI RMF by organizations is voluntary, and it was designed to be applicable to all industry sectors and to give AI stakeholders and users approaches that increase the trustworthiness of AI systems.

NIST intends for the AISIC to leverage NIST's history of collaborating with the private and public sectors to develop reliable and practical measurement and standards-oriented solutions. Specifically, NIST expects the AISIC to:

Establish a knowledge and data sharing space for AI stakeholders

Engage in collaborative and interdisciplinary R&D through a Research Plan

Prioritize research and evaluation requirements and approaches that allow for a more complete and effective understanding of AI's impacts on society and the US economy

Identify and recommend approaches to facilitate the cooperative development and transfer of technology and data between and among AISIC members

Identify mechanisms to streamline input from federal agencies on topics within their direct purviews

Enable assessment and evaluation of test systems and prototypes to inform future AI measurement efforts

AISIC working groups

NIST hosted the first USAISI workshop on November 17, 2023, with a focus on AI safety. Based on that workshop, NIST created five working groups for AISIC members:

Working Group #1: Risk Management for Generative AI

Working Group #2: Synthetic Content

Working Group #3: Capability Evaluations

Working Group #4: Red-Teaming

Working Group #5: Safety & Security

The specific areas of focus for each working group are listed here.

Where are the state government stakeholders?

The AISIC's membership list does not mention any state governments or state legislative organizations. Additionally, the objectives NIST identified above mention federal agencies but not state governments. To the extent that state legislatures and municipal entities are enacting legislation, it would be wise for the AISIC to engage with state governments. Otherwise, we run the risk of another patchwork of legislation akin to the data breach notifications and privacy laws that filled the void left by the U.S. Congress.

Conclusion

Legislators, regulators, and vendors are filling the airwaves with AI topics. Industry commentators often describe the NIST Cybersecurity Framework as one of the most reliable security measures to develop and deploy a program. Skeptics paradoxically claim it is not comprehensive or is too complicated for senior leaders and board members to digest. The ultimate challenge for the AISIC may be to work quickly enough to stay abreast of AI's adoption in the marketplace while striking the right balance between complexity and simplicity—in other words, the members may have volunteered to solve a Wicked Problem.