wiley

NEWSLETTER

AI Risk Management Framework Is Among Emerging Federal Initiatives on AI

—

September 2021

Privacy In Focus®

Artificial intelligence (AI) has drawn significant policy interest for quite some time now, and a federal approach is taking shape. A recent flurry of federal activity on the AI front has emanated in large part from the U.S. Department of Commerce (Commerce) – including a move towards development of a risk management framework. The framework in particular may greatly influence how companies and organizations approach AI-related risks, including avoiding bias and promoting accuracy, privacy, and security.

Developing an AI Risk Management Framework

In the National Defense Authorization Act for Fiscal Year 2021 (2021 NDAA), Congress directed the National Institute of Standards and Technology (NIST) – which falls under Commerce – to develop "a voluntary risk management framework for trustworthy [AI] systems." Following this directive, in late July, NIST issued a Request for Information (RFI) seeking input to help inform the development of what it refers to as the AI Risk Management Framework (AI RMF).

As NIST explained, the AI RMF is "intended to help designers, developers, users, and evaluators of AI systems better manage risks across the AI lifecycle" and "aims to foster the development of innovative approaches to address characteristics of trustworthiness," including accuracy and mitigation of harmful bias. According to NIST, the development of the AI RMF "will involve several iterations to encourage robust and continuing engagement and collaboration with interested stakeholders" and "will include open, public workshops, along with other forms of outreach and feedback."

Authors
—

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas
—

Artificial Intelligence (AI)
Privacy, Cyber & Data Governance

In the RFI, NIST proposed that the AI RMF should feature eight key attributes. Specifically, NIST explained that the AI RMF should:

- "Be consensus-driven and developed and regularly updated through an open, transparent process";
- "Provide common definitions" for terms like "trust" and "trustworthiness";
- "Use plain language that is understandable by" and useful to "a broad audience";
- "Be adaptable to many different organizations, AI technologies, lifecycle phases, sectors, and uses";
- "Be risk-based, outcome-focused, voluntary, and non-prescriptive";
- "Be readily usable as part of any enterprise's broader risk management strategy and processes";
- "Be consistent, to the extent possible, with other approaches to managing AI risk"; and
- "Be a living document.**"**

This directive – as well as NIST's RFI outlining the initial attributes and goals of the AI RMF – aligns with NIST's extensive work on similar frameworks for cybersecurity and privacy.

The RFI is the beginning of the collaborative development process at NIST with respect to the AI RMF. In the immediate near term, NIST is hosting a public workshop on October 19-21, 2021 to share feedback received in response to the RFI and discuss plans and goals for the AI RMF.

The National Artificial Intelligence Advisory Committee

On September 8, Secretary of Commerce Gina Raimondo announced that Commerce would be establishing a National Artificial Intelligence Advisory Committee (NAIAC) pursuant to a separate directive from the 2021 NDAA. The NAIAC, which will also include a subcommittee focused on the use of AI in law enforcement, will provide recommendations to the President on a broad range of AI-related topics, including the United States' competitiveness in the AI space, the state of science related to AI, AI workforce issues, and opportunities for international AI cooperation.

NIST has already issued a Federal Register notice formally calling for nominations to the NAIAC. As this notice explains, the NAIAC will consist of at least nine members representing academia, industry, nonprofits, and federal laboratories who will be tasked with submitting a report to the President and Congress within one year, and then once every three years thereafter. Nominations for the NAIAC are due October 25, 2021.

Looking Ahead

These recent developments coming out of Commerce are by no means the only federal AI actions that have been taken since President Biden assumed office. For example, the Biden Administration launched AI.gov in May in order to introduce more Americans to the government's activities in the AI space. Similarly, in June, the White House Office of Science and Technology Policy and the National Science Foundation established a National Artificial Intelligence Research Resource Task Force that will help to expand access to educational tools and resources in order to spur AI innovation.

Given the responsibilities that have been assigned to it and the actions that it has already taken, Commerce – and NIST in particular – appears poised to be central to the federal government's approach. As such, stakeholders should consider engaging with NIST in its AI workstreams, including through participation in the upcoming workshop.

***

Our Artificial Intelligence Practice counsels clients on AI compliance, risk management, and regulatory and policy approaches, and we engage with key government stakeholders, including NIST, in this quickly moving area. Please reach out to a member of our team with any questions.

© 2021 Wiley Rein LLP