wiley

NEWSLETTER

Federal AI Efforts Will Be Greatly Boosted by 2021 NDAA

January 2021

Privacy In Focus®

The National Defense Authorization Act for the Fiscal Year 2021 (2021 NDAA) – which was passed over a Presidential veto on January 1– represents a massive step forward for American AI policy in areas far beyond national defense. It incorporates a number of AI legislative proposals that will reshape the government's approach over the next two years, as part of a broader emphasis on promoting emerging technologies.

Among its many elements, the 2021 NDAA (1) expands National Institute of Standards and Technology's (NIST) AI responsibilities, including directing it to establish a voluntary risk management framework–in consultation with industry–that will identify and provide standards and best practices for assessing the trustworthiness of AI and mitigating risks from AI systems; (2) launches the National Artificial Intelligence Initiative, setting up a federal bureaucracy designed to deal both with agencies and outside stakeholders, as well as advise on key issue issues of AI implementation like bias and fairness; (3) gives the Department of Defense (DoD) specific authority to procure AI while requiring an assessment meant to promote acquisition of AI that is "ethically and responsibly developed." All of these initiatives will have ripple effects on private sector development, testing, and deployment of AI systems–and heavily influence regulatory expectations on issues like AI bias, accuracy, and security.

Below is a high-level summary of these key AI provisions.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Associate
202.719.7577
kscott@wiley.law

Practice Areas

Artificial Intelligence

NIST Is Required to Development a Risk Management Framework for Use in Implementing AI

The NDAA gives NIST specific direction and deadlines for developing a risk management framework for use of AI and defining measurable standards that can be used within the framework. NIST already has been very active on AI issues, particularly following the 2019 AI Executive Order. The NDAA expands NIST's AI responsibilities through a specific legislative mandate on AI, placing the agency at the center of working through critical issues involving bias, privacy, security, transparency, and even ethics. And while this directive will result in a risk framework that will be voluntary, NIST's work in similar areas like cybersecurity has proven enormously influential to the private sector and has been closely monitored by policymakers.

Specifically, the NDAA amends the National Institute of Standards and Technology Act to give NIST four distinct missions with respect to AI:

- Advancing collaborative frameworks, standards, guidelines, and associated methods and techniques for AI;
- Supporting the development of a risk-mitigation framework for deploying AI systems;
- Supporting the development of technical standards and guidelines that promote trustworthy AI systems; and
- Supporting the development of technical standards and guidelines by which to test for bias in AI training data and applications.

It directs NIST to develop an AI risk management framework within two years. The framework must include standards, guidelines, procedures, and best practices for developing and assessing "trustworthy" AI and mitigating risks related to AI. NIST also must establish common definitions for elements of trustworthiness, including explainability, transparency, safety, privacy, security, robustness, fairness, bias, ethics, validation, verification, and interpretability. This mandate aligns with NIST's ongoing work regarding trustworthy AI, but importantly, it provides a more definite timeline and specific elements for the framework. It also makes clear that NIST should work to develop common definitions related to a range of complex issues like bias and transparency—and even ethics and fairness, which are not usually within NIST's ambit—that could have broader implications if adopted by regulatory bodies concerned with potential adverse effects of AI.

Additionally, the NDAA requires NIST—within a year—to develop guidance to facilitate the creation of voluntary AI-related data sharing arrangements between industry and government, and to develop best practices for datasets used to train AI systems, including standards for privacy and security of datasets with human characteristics. The guidance around datasets will have particular importance for mitigating bias that can result from AI making use of data that is not representative.

NIST has a long history of collaborating with industry stakeholders on key issues, including cybersecurity and privacy, and its AI work to date has followed this collaborative approach. Indeed, NIST is planning a virtual workshop on Explainable AI later this month. With NIST's newly expanded role, AI stakeholders will have multiple additional opportunities to engage.

The National Artificial Intelligence Initiative Is Launched with a New Bureaucratic Framework.

The NDAA instructs the President to establish the ''National Artificial Intelligence Initiative'' and provides a framework for its implementation throughout the federal government. The focus of this Initiative will be to ensure continued U.S. leadership in AI R&D and the development and use of "trustworthy artificial intelligence systems;" to prepare the U.S. workforce for integration of AI; and to coordinate AI R&D among civilian, defense, and intelligence agencies.

To implement the Initiative, the law establishes a bureaucratic framework for dealing with AI within the government, complementing efforts that previous Administrations have made without a legislative mandate. These include:

- ***The National Artificial Intelligence Initiative Office.*** This Office will be housed within the White House's Office of Science and Technology Policy (OSTP) and will serve as an external and internal contact on AI, conduct outreach, and act as agency hub for technology and best practices.
- ***An AI Interagency Committee.*** The Interagency Committee—to be co-chaired by the Director of the OSTP and, on an annual rotating basis, a representative from the Department of Commerce, the National Science Foundation, or the Department of Energy—will coordinate Federal programs and activities in support of the National Artificial Intelligence Initiative.
- ***The National Artificial Intelligence Advisory Committee.*** This Advisory Committee—to be established by the Department of Commerce in consultation with a slate of other federal stakeholders—will include members with broad and interdisciplinary expertise and perspectives, including from academic institutions, nonprofit and civil society entities, Federal laboratories, and companies across diverse sectors. It will provide recommendations related to, among other things, "whether ethical, legal, safety, security, and other appropriate societal issues are adequately addressed by the Initiative," and "accountability and legal rights, including matters relating to oversight of AI using regulatory and nonregulatory approaches, the responsibility for any violations of existing laws by an AI system, and ways to balance advancing innovation while protecting individual rights." It also will include a subcommittee on AI in law enforcement that will advise on issues of bias (including use of facial recognition), security, adoptability, and legal standards including privacy, civil rights, and disability rights.

This Initiative also presents an opportunity for private sector engagement. The Initiative's many priorities include coordinating R&D and standards engagement and providing outreach to diverse stakeholders, including citizen groups, industry, and civil rights and disability rights organizations. In particular, the National Artificial Intelligence Advisory Committee is required to include industry representatives as it makes recommendations on key issues including AI oversight by the government.

DoD Is Directed to Assess Its Ability to Acquire Ethically and Responsibly Developed AI Technology.

The NDAA provides the Department of Defense's (DoD) Joint Artificial Intelligence Center (JAIC) with authority to acquire AI technologies in support of defense missions. Additionally, it puts into place procedures to ensure that DoD acquires AI that is "ethically and responsibly developed" and that it effectively implements ethical AI standards in acquisition processes and supply chains.

Specifically, the NDAA requires the Secretary of Defense to conduct an assessment to, among other things, determine whether DoD has the ability, resources, and expertise to ensure that the AI it acquires is ethically and responsibly developed. The assessment must be completed within 180 days, and following that, the Secretary must brief the Congressional committees as to the results.

These provisions will impact DoD procurement and contractors, and given the size and scope of the Defense acquisition budget, will also likely impact private sector development of AI to meet "ethical and responsible" standards.

***

AI technology has been an area of increased focus of the federal government in the past several years, most notably following 2019 and 2020 AI Executive Orders. The new efforts launched by the 2021 NDAA add to existing work and make clear that AI will be a continued focus of federal government activity.

Our Artificial Intelligence Practice counsels clients on AI compliance, risk management, and regulatory and policy approaches, and we engage with key government stakeholders in this quickly moving area. Please reach out to one of the authors of this article with any questions.