LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Biden's AI Guidance For Gov't May Need More Risk Controls

By **Daniel Wilson**

Law360 (May 3, 2024, 9:36 PM EDT) -- The Biden administration's latest guidance for federal agencies' purchases of generative artificial intelligence technologies doesn't fully account for risks such as systems failing to work as intended, and could therefore fail to deter agencies from ill-advised investments, according to experts.

In an effort to regulate the responsible use of the emerging technology, which can create new content such as text or video, the General Services Administration recommended that agencies looking into buying generative AI services and related hardware should weigh the technology's benefits — such as being able to automatically respond to questions from the public — against risks, such as inaccurate responses to those questions.

But experts say the broad, high-level guidance is more of a primer than a comprehensive guide that neither fully explains nor accounts for potential risks posed by generative AI, such as nonsensical output from algorithms misinterpreting data, nor explicitly lays out appropriate and inappropriate use cases.

That means that agencies' potential interest in using "a bright and shiny toy" might not be appropriately tempered by considerations of risk when determining whether to use generative AI, said Alex Major, co-chair of the government contracts group at McCarter & English LLP, whose practice often involves cybersecurity and data privacy risk issues.

"It's really an attractive nuisance in a lot of ways," he said. "And because of that, the guardrails, just like with any attractive nuisance ... need to be very, very clearly identified for the government. These tools are so incredibly dynamic, not taking the time to put in [specific] guardrails is, I think, beyond risky."

For example, there is no specific accounting in the guidance for what to do if a generative AI system purchased by an agency isn't working well or has otherwise "gone off the rails," noted Holland & Knight LLP partner Paul Stimers, whose practice focuses on emerging technology issues.

"I don't know if that was just a blind spot or if that was, to some degree, a [deliberate] decision," Stimers said. "This is, in part, a political document — not a partisan document, but a document that is laying out a net positive message about AI to the federal government."

Some of the advice the GSA has provided to agencies may also be directly counterproductive to its stated goal of encouraging responsible and effective use of generative AI, such as the suggestion that agencies consider using publicly available web-based AI tools for some of their needs, said Michelle

Coleman, a Crowell & Moring LLP partner who often advises clients on AI-related issues.

"I'm surprised that the government would offer that as something that an agency should consider using, just because there's so much risk to including the information that you might need to get the output that you want from generative AI, and that information being confidential to the government or something that shouldn't be shared with the general public, and certainly not used to continuously train those public websites," she said.

Also, although the guidance touches on the issue of ownership of data as a consideration for agencies to take into account when contemplating generative AI, it doesn't explicitly address how agencies should resolve issues related to data rights, which may dampen the desire of potential contractors to work with agencies on those systems.

Government demands for extensive data rights have long been a bugbear for contractors, such as when the government seeks technical data from an original equipment manufacturer so that it can tap other contractors to make spare parts.

Data rights are particularly pertinent for generative AI systems, which rely on extensive amounts of underlying data to feed the algorithm and then themselves generate entirely new data. Determining who owns what is likely to be "messy" — particularly if an AI system is being sold to the government through a reseller and not directly by the generative AI company itself, said Sheppard Mullin Richter & Hampton LLP partner Townsend Bourne, who specializes in data protection and technology-related issues.

"[Agencies] really need to iron out data rights issues up front," she said.

There are some more descriptive aspects of the guidance, however, that can meaningfully help agencies in determining whether using generative AI makes sense for their needs, such as the GSA's suggestion that agencies use a "sandbox" — a type of small-scale, low-cost technology test bed — before committing to any full-scale purchase of an AI system, McCarter & English's Major said.

"The concept of sandboxes, I think, will be super helpful," he said. "'How can we use this technology? What should we be using it for?' I think that should be mandatory, before any agency even uses [generative AI]."

Sandboxes not only give agencies a way to test a system's security and usability in a controlled environment, but also give companies that offer generative AI solutions a potential foot in the door for working with the government, according to Major.

"I think it would be very wise for contractors to offer that option," he said. "'We understand AI is confusing, we suggest using it here — come play on our system for a little bit.'"

--Editing by Alanna Weissman and Emily Kokoll.
