

Privacy Daily

Under the terms of your subscription agreement, you may print one copy of an individual article for your own use. Please respect that limit.

June EO a 'Continuation' of White House Approach to AI, Lawyer Says

June 25, 2026 by Kara Thompson

The Trump administration's executive order on June 2 asking AI developers to voluntarily share models with the federal government before they're released (see 2606020061) demonstrates the White House is walking the line between protecting innovation and instituting guardrails, said Erin Prest, cybersecurity and data privacy lawyer at McCarter & English.

She told *Privacy Daily* in an interview that she saw significance both in what was included in the order and what was left out. One of the "important" things the EO does is establish a process for people to submit models to the government for review, though this is "voluntary" and "not mandatory," Prest said.

The voluntary review "is one of the more noteworthy aspects" of the order, blogged Morrison Foerster lawyers earlier in June. The EO "makes clear that it does not authorize any mandatory preclearance or licensing regime," they said. But "early engagement may offer certain practical advantages," such as building credibility and the opportunity to engage with the government.

On the other hand, privacy isn't mentioned in the order, Prest said. But her "read" is that government agencies using a company's AI tool will "probably end up doing a privacy impact assessment" (PIA) anyway because of other statutes, like the E-Government Act of 2002, even though PIAs aren't mentioned specifically in the EO.

"You wouldn't need to call it out specifically in order for it to happen," she said, "it's already ... kind of baked in." Prest noted that the DOJ has revised its PIA templates to include specific questions about AI and machine learning as evidence that "while AI is new, it's just a new flavor ... of things that already exist," and existing guidelines and parameters can be applied to the new piece.

The EO did, however, "specifically [call] out the protection against criminal actors," Prest said. She wasn't sure that this was necessary, as like PIAs, it would still exist without a specific mention in the order. But "by actually calling that piece out, they really are trying to ... put people on notice" and remind them that "if you are doing this for illegal purposes or criminal acts, you are going to be a focus."

Cooley lawyers highlighted that the EO "does not create new civil liability," nor does it "address AI governance beyond the cybersecurity context."

Prest applauded the administration for doing a "good job in keeping [the EO] short and to the point," so that it's "easy to read and understand."

Overall, the order is “company and invention-friendly in terms of setting some guardrails” and “putting some parameters around [AI] without overly stifling innovation,” Prest said. But the “devil’s in the details,” she said, so it’ll be “interesting” to see how it plays out.

Time Will Tell

The EO is a “continuation” of what the White House has already said about AI, Prest said. “It shows that the administration is continuing to think about AI and innovation,” but it’s taking steps, instead of “pushing something out to have something out.”

There are also some aspects of the order that are “murky,” she said. For example, the benchmarking that determines whether a particular model is covered “is classified.” Because of this, “it will be interesting to see what information companies get back” about “why their models either are or are not covered.”

She’s also eager to see “what exactly is the government doing when it’s reviewing” the models, as right now it “seems a little up in the air.”

For companies developing AI models and tools, Prest recommended “taking a hard look” to determine inherent or potential risks, or if there are areas where extra protections or guardrails should be implemented.

The Morrison Foerster lawyers also recommended AI developers monitor forthcoming federal guidance on what counts as a covered model as well as the collaboration framework. Additionally, developers should be proactive in assessing whether current or planned models fall within the EO’s scope, review cybersecurity practices and update any contractual obligations and protections as needed.

AI deployers, too, should review contracts with AI providers, consider incident-response protocols and track future federal guidance and definitions around the AI space, the blog added.

Not Far Enough

A couple technology groups and a member of Congress praised certain aspects of the EO, but they slammed the order for being too little too late.

The administration “has belatedly discovered the need to redo something it hastily dismantled in its first year,” said Sen. Mark Warner, D-Va., in a press release following the EO’s announcement. He called the order a “course correction” that “rehash[es]” proposals from a 2023 Biden executive order, “bipartisan congressional legislation, and each of the last three years of intel authorization bills the Senate Intel Committee has passed.”

Though the order “can begin to grapple with widespread impacts that new frontier

models will have on our critical infrastructure, it can't undo the years wasted on dismantling some of the most vital pillars of our nation's cybersecurity response," he added.

Warner, however, "salute[d]" the inclusion of "pre-deployment testing on a collaborative basis," and added he was "strongly supportive" of the National Security Agency evaluating national security implications of frontier AI models.

Trade association NetChoice, too, supported the "pro-innovation and growth agenda," but raised concerns that "some of the powers and vagueness, as well as the overall precedent of the Order, could be misused in the hands of a future administration."

In a press release, NetChoice Director of Policy Patrick Hedger celebrated Trump's "light-touch and collaborative approach," but said the association is "concerned that future administrations won't honor his vision," citing previous threats against and pressure of social media companies as proof.

"Unless further guardrails against this kind of graft are put in place or Congress finally acts to deliver a national AI framework, we are concerned the collaborative framework President Trump has put forward will not remain voluntary," he added.

The Center for Democracy and Technology also applauded some aspects of the order while raising concerns as well.

The EO "takes steps to address" the threats that "advanced artificial intelligence models pose ... to the integrity of the companies and critical infrastructure on which we all rely," said Samir Jain, CDT vice president of policy, in an emailed press statement. It "further attempts to avoid the deeply concerning implications of a mandatory licensing regime for release of new models," he added, celebrating the testing and benchmarking programs that are "important to promote cybersecurity and address other risks."

Despite this, Jain said the order "should not become a mechanism for the Administration to punish companies for political or other arbitrary reasons," noting that CDT "will be closely monitoring the details of its implementation as they emerge."

Copyright© 2026 by Warren Communications News, Inc. Reproduction or retransmission in any form, without written permission, is a violation of Federal Statute (17 USC101 et seq.). Please review our [User Agreement](#).