MINTZ

Biden's AI Executive Order Achieves First Major Milestones (AI EO January Update) — AI: The Washington Report

February 02, 2024 | Article | By **Bruce D. Sokler**, **Alexander Hecht**, **Christian Tamotsu Fjeld**, Raj Gambhir

VIEWPOINT TOPICS

- Artificial Intelligence
- Antitrust
- ML Strategies

RELATED PRACTICES

- Antitrust
- Lobbying and Public Policy

RELATED INDUSTRIES

On January 29, 2024, the White House published a **fact sheet** detailing the actions that have been taken pursuant to President Joe Biden's October 30, 2023 executive order on "**Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**" ("AI EO"). As covered in our **timeline of the executive order**, a number of provisions were scheduled to come into effect by the January 28, 2024 deadline. According to the White House's announcement, more than two dozen actions pursuant to the executive order have been completed so far.

In this week's newsletter, we will cover five major provisions enacted since October 2023. Our key takeaways are:

1. According to the White House, federal agencies have so far met "all of the 90-day actions" set by the AI EO.
2. Some important actions taken so far include a Defense Production Act (DPA) **determination on AI safety test results**, **Commerce Department draft rules** on US-based Infrastructure as a Service (IaaS) firms, a **launch of the National AI Research Resource** (NAIRR) pilot, the Federal Trade Commission's ("FTC" or "Commission") **proposed update to the Children's Online Privacy Protection Act** (COPPA) Rule, and the launch of a **federal AI hiring spree**.
3. **More deadlines** set by the AI EO are coming at the end of February and March. The April 27, 2024, deadline will be particularly consequential, as 30 actions implicating agencies across the federal bureaucracy will be due that day. We will continue to cover developments related to the AI EO as they arise.

In This Edition

Defense Production Act Determination on AI Safety Test Results

Commerce Department Issues Draft Rule on Infrastructure as a Service Companies

National Science Foundation Launches Pilot of National AI Research Resource

Federal Trade Commission Proposes First COPPA Rulemaking in a Decade

AI Talent Surge Kicks Off

Conclusion: April on the Horizon

Action	Agency	Required Timeline	
Evaluated ways to prioritize agencies' adoption of AI through the Technology Modernization Fund	Technology Modernization Board	30 days	COMPLETE
Directed the Nontraditional and Emerging Transportation Technology Council to evaluate the transportation sector's need for AI guidance and technical assistance	Department of Transportation	30 days	COMPLETE
Reported federal agency resources available to incorporate into the National AI Research Resource (NAIRR) pilot	Agencies identified by the National Science Foundation	45 days	COMPLETE
Identified priority areas for increasing federal agency AI talent and accelerated hiring pathways	Office of Science and Technology Policy & Office of Management and Budget	45 days	COMPLETE
Convened AI and Tech Talent Task Force	White House Chief of Staff's Office	45 days	COMPLETE
Launched an AI Talent Surge to accelerate hiring AI professionals across the federal government, including through a large-scale hiring action for data scientists	Agencies coordinating with the AI and Tech Talent Task Force	45 days	COMPLETE
Published a Request for Information (RFI) on whether to revise the list of Schedule A job classifications that do not require permanent labor	Department of Labor	45 days	COMPLETE

CLICK TO VIEW FULL SIZE

*Actions pursuant to the AI EO completed as of January 29, 2024. (**Source**)*

Defense Production Act Determination on AI Safety Test Results

Over the past few years, **experts have warned** that powerful AI tools could pose "potentially catastrophic effects on society" if not properly regulated. For instance, rogue autonomous systems "**could facilitate the creation of novel bioweapons** and lower barriers to obtaining such agents." AI models that have the capacity to show "high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety" are referred to in the AI EO as "dual-use foundation models."**[1]**

Pursuant to the Defense Production Act, the AI EO directs the Secretary of Commerce to require companies "developing or demonstrating an intent to develop potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records" related to the following information:

- "any ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats"
- "the ownership and possession of the model weights**[2]** of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights"
- "the results of any developed dual-use foundation model's performance in relevant AI red-team testing…"**[3]**

The White House's January 2024 **fact sheet** on the implementation of the AI EO announced that the Defense Production Act has been invoked to "compel developers of the most powerful AI systems to report vital information, especially AI safety test results, to the Department of Commerce."**[4]** As Ben Buchanan, a White House special adviser on AI put it in a **statement to the press**, regulatory authorities want "to know AI systems are safe before they're released to the public — the president has been very clear that companies need to meet that bar."

Commerce Department Issues Draft Rule on Infrastructure as a Service Companies

On January 29, 2024, the Commerce Department published a proposed rule concerning US-based Infrastructure as a Service (IaaS) providers and their foreign resellers entitled, "**Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities**."

The Commerce Department promulgated the proposed rule pursuant to the **AI EO's** requirement that the Commerce Secretary propose "regulations that require United States IaaS Providers to submit a report to the Secretary of Commerce when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity," among other requirements.

IaaS providers allow customers to access computing resources, usually over the cloud. As discussed in our newsletter on AI and chips, cloud computing services allow firms that do not have access to sufficient computing resources to develop their own powerful AI models. The proposed Commerce Department rule is intended to ensure that malign entities cannot circumvent **US trade restrictions, principally on powerful chips**, to develop advanced AI models.

The proposed rule would require that US-based IaaS providers and their foreign resellers ("providers") "verify the identity of foreign customers." Providers would be required to "report to the Department [of Commerce] when they have knowledge they will engage or have engaged in a transaction with a foreign person that could allow that foreign person to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity."

The Secretary of Commerce would be granted the power to "prohibit or impose conditions on the opening or maintaining with any U.S. IaaS provider of an Account, including a Reseller Account, by any foreign person located in a foreign jurisdiction found to have any significant number of foreign persons offering U.S. IaaS products used for malicious cyber-enabled activities, or by any U.S. IaaS provider of U.S. IaaS products for or on behalf of a foreign person."

This rule can be understood as an escalation of the United States' strategic competition with the People's Republic of China (PRC) regarding the development of advanced technologies. If implemented as written, this rule would complement restrictions on the sale of advanced semiconductors to the PRC, limiting options for PRC firms to access the hardware requisite to develop leading-edge AI models.

Comments on this rule can be submitted through the ***Federal Register*'s online portal**. The comment period for this proposed rule closes on April 29, 2024.

National Science Foundation Launches Pilot of National AI Research Resource

A major accomplishment of the AI EO has been the National Science Foundation's (NSF) launch of the **National AI Research Resource** (NAIRR) pilot.

In June 2020, Representative Anna Eshoo (D-CA-16) introduced the **National AI Research Resource Task Force Act**, a bill that would establish a task force to "investigate the feasibility and advisability of establishing a national artificial intelligence research resource" and "propose a roadmap detailing how such resource should be established and sustained." Congress folded the bill into the National Defense Authorization Act of 2021, and by June 2021, the NAIRR Task Force had formally launched.

For over two years, the NAIRR Task Force constructed a proposal for the NAIRR. Their work culminated in their **January 2023 final report**. The report forcefully advocated for the NAIRR, stating that the resource "would transform the U.S. national AI research ecosystem and facilitate the ability to address societal-level problems by strengthening and democratizing participation in foundational, use-inspired, and translational AI R&D in the United States." In the months following the issuance of the report, prominent AI firms and research institutions **voiced their support** for the NAIRR Task Force's proposal.

In response to these developments, the AI EO orders the Director of the NSF to "launch a pilot program implementing the [NAIRR], consistent with past recommendations of the NAIRR Task Force." On January 24, 2024, the NSF fulfilled this requirement by **formally announcing the launch of the NAIRR pilot**. At the time of writing, NAIRR has eleven government partners, including the Departments of Energy (DOE) and Defense (DoD), the National Institutes of Health (NIH), and the Defense Advanced Research Projects Agency (DARPA).

The pilot also has 25 private sector, nonprofit, and philanthropic partners, including the largest digital technology and AI firms in the United States. The NSF's announcement states that the NAIRR pilot is seeking additional private sector and nonprofit partners and that interested parties should **email NAIRR** for further details.

The NAIRR pilot will have four primary initiatives:

1. **NAIRR Open**: NAIRR will provide access to AI research resources.
2. **NAIRR Secure**: Under the direction of the NIH and the DOE, NAIRR will coordinate research and resources on the strengthening of digital privacy and security.
3. **NAIRR Software**: NAIRR will "facilitate and investigate inter-operable use of AI software, platforms, tools and services?for NAIRR pilot resources."

4. **NAIRR Classroom**: NAIRR will conduct outreach efforts to members of the public to encourage the use of NAIRR resources and the development of AI more generally.

As of January 2024, the NAIRR pilot has launched two programs.

Advanced Computing Allocations to Advance AI Research and Education

On January 24, 2024, the NSF and DOE **announced a research call** to all "meritorious advanced computing proposals by US-based researchers and educators." Selected projects will receive access to computational resources provided by NAIRR partners, such as the DOE's Oak Ridge National Laboratory **Summit supercomputing system**.

Researchers must submit an application detailing a project "focused on advancing Safe, Secure and Trustworthy AI," such as an intervention for "assuring that model functionality aligns with societal values and obeys safety guarantees."

Applicants have until 8:00 pm EDT on March 1, 2024, to submit their applications. For more information, please visit the **research call web portal**.

Publicly Accessible Resources for AI Development

The NAIRR pilot has compiled "**government and non-government contributed resources** aligned with the NAIRR Pilot goals, such as pre-trained models, AI-ready datasets, and relevant platforms." At the time of writing, the pilot resources page lists over a dozen resources from NAIRR partners such as DoD, DOE, and NIH. More resources are expected to be added in the coming months.

Federal Trade Commission Proposes First COPPA Rulemaking in a Decade

As discussed in our **newsletter on the AI EO**, the order explicitly encourages the FTC to consider whether to exercise its rulemaking authority "to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI." Pursuant to this order, on December 20, 2023, the **FTC announced a rulemaking concerning the Children's Online Privacy Protection Act** (COPPA). COPPA is a 1998 law empowering the FTC to regulate the collection of children's data by online services.

The proposed December 2023 rule would expand the scope of practices barred under COPPA, limit exceptions, and subject entities participating in Safe Harbor programs to greater scrutiny. "By requiring firms to better safeguard kids' data, our proposal places affirmative obligations on service providers and prohibits them from outsourcing their responsibilities to parents," **commented FTC Chair Lina Khan** in reference to the proposed rule. If instituted, this proposed rule would constitute the **first change to the COPPA Rule since 2013**.

Provisions of the proposed rule include:

- **Opt-in for targeted advertising**: Covered online services would be "**required to obtain** separate verifiable parental consent to disclose information to third parties including third-party advertisers — unless the disclosure is integral to the nature of the website or online service."
- **Prohibition on collecting more data than is reasonably necessary**: The rule would expand the existing limitation on conditioning children's access to a service on data collection, making it an "**outright prohibition** on collecting more personal information than is reasonably necessary for a child to participate in a game, offering of a prize, or another activity." This prohibition would apply "**even if the operator obtains consent** for the collection of information that goes beyond what is reasonably necessary."
- **Limiting the internal operations exception**: Currently, COPPA allows operators to collect children's **persistent identifiers**, or data "that can be used to recognize a user over time and across different websites or online services," under a so-called "internal operations exception." This exception applies as long as operators are collecting persistent identifiers for the "**sole purpose** of providing support for the internal operations of the website or online service." The proposed rule would require "operators utilizing this exception to **provide an online notice** that states the specific internal operations for which the operator has collected a persistent identifier and how they will ensure that such identifier is not used or disclosed to contact a specific individual, including through targeted advertising."
- **Circumscribing the digital "nudging" of children**: The rule would prohibit operators from using contact information or persistent identifiers to send notifications to children "**to encourage or prompt use** of the operator's website or online service," a technique commonly known as "nudging."
- **Codifying guidance on Ed Tech**: The rule would codify elements of the Commission's May 2022 "**Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act**" by allowing "schools and school districts to authorize ed tech providers to collect, use, and disclose students' personal information but only for a school-authorized educational

purpose and not for any commercial purpose."

- **Increasing transparency requirements for COPPA Safe Harbor programs**: The rule would **require COPPA Safe Harbor programs** to expand their annual reports to include "each subject operator and all approved websites or online services in the program, as well as all subject operators that have left the program…a narrative description of the program's business model…a description of the process for determining whether a subject operator is subject to discipline" and more.
- **Strengthening data security requirements**: The rule would require that "operators establish, implement, and maintain a **written children's personal information security program** that contains safeguards that are appropriate to the sensitivity of the personal information collected from children."
- **Limiting data retention**: The rule would establish that operators may only retain personal information "for as long as necessary to fulfill the specific purpose for which it was collected." Accordingly, operators would not be allowed to use personal information for secondary purposes or retain personal information indefinitely.

The comment period for the proposed rule closes on March 11, 2024. Comments can be submitted through the ***Federal Register*'s online portal**.

AI Talent Surge Kicks Off

To build administrative capacity to address the challenges posed by AI, **the AI EO** calls for a cross-agency hiring surge to increase "AI talent in the Federal Government." According to the White House's January 2024 **fact sheet** on the implementation of the AI EO, the "Office of Personnel Management has granted flexible hiring authorities for federal agencies to hire AI talent, including direct hire authorities and excepted service authorities." Additionally, existing government-wide tech talent programs such as Presidential Innovations Fellows and the US Digital Corps have scaled up hiring for AI talent in 2024 across "high-priority AI projects."

Interested applicants should visit the federal government's **AI talent hub** to explore job openings and other relevant opportunities.

Conclusion: April on the Horizon

While January 2024 saw the completion of many actions ordered by the AI EO, **the most consequential deadline**, April 27, 2024, is still on the horizon. There are 30 tasks due on the April deadline alone, not to mention the almost a dozen actions due in late February and March. These actions implicate agencies across the federal bureaucracy and touch on a wide swath of topics, including copyright, civil rights, national defense, and immigration. While January has been a busy month in Washington, as far as federal actions on AI go, the year is just getting started.

We will continue to monitor, analyze, and issue reports on these developments. Please feel free to contact us if you have questions as to current practices or how to proceed.

Endnotes

---

[1] A model must also be "trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts" to fall under the AI EO's definition of "dual-use foundation model."

[2] Model weights are the parameters that constitute some AI models. During the training process, model weights are adjusted iteratively until the AI model achieves a sufficient degree of accuracy, usefulness, or both.

[3] As explained in our **July 2023 newsletter** on Biden's voluntary framework on AI, "**red-teaming**" is "a strategy whereby an entity designates a team to emulate the behavior of an adversary attempting to break or exploit the entity's technological systems. As the red team discovers vulnerabilities, the entity patches them, making their technological systems resilient to actual adversaries."

[4] At the time of writing, the text of the presidential determination on the use of the DPA to compel certain AI developers to provide reports on dual-use foundational models has not yet been released.

Authors

Bruce D. Sokler, Member / Co-chair, Antitrust Practice

Bruce D. Sokler is a Mintz antitrust attorney. His antitrust experience includes litigation, class actions, government merger reviews and investigations, and cartel-related issues. Bruce focuses on the health care, communications, and retail industries, from start-ups to Fortune 100 companies.

Alexander Hecht, ML Strategies - Executive Vice President & Director of Operations

Alexander Hecht is Executive Vice President & Director of Operations of ML Strategies, Washington, DC. He's an attorney with over a decade of senior-level experience in Congress and trade associations. Alex helps clients with regulatory and legislative issues, including health care and technology.

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm's Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Raj Gambhir

Raj Gambhir is a Project Analyst in the firm's Washington DC office.

More Viewpoints

Algorithmic Disgorgement: An Increasingly Important Part of the FTC's Remedial Arsenal — *AI: The Washington Report*

January 24, 2024 | Article | By **Bruce Sokler**, **Alexander Hecht**, **Christian Tamotsu Fjeld**, Raj Gambhir

Read more