

Timeline: Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence

By [Shiva Aminian](#), [Jingli Jiang](#), [Natasha Kohne](#), [Susan Lent](#), [Ed Pagano](#), [Michelle Reed](#), [Hans Rickhoff](#), [David Vondle](#), [Reggie Babin](#), [Casey Higgins](#), [Ryan Thompson](#), [Alan Hayes](#), [Maka Hutson](#), [Thomas Krueger](#) and [Taylor Daly](#)

November 10, 2023

On October 30, 2023, the Biden administration issued its long-awaited artificial intelligence (AI) executive order (EO), which issues directives to over 20 federal agencies, with the deadline for implementation spanning between 30 and 365 days—just ahead of the 2024 election (see prior alert [here](#)).

The EO was quickly followed by the Office of Management and Budget’s (OMB) release of **draft guidance** for public comment on federal agencies’ use of AI, granting stakeholders until December 5, 2023, to provide feedback.

The U.S. Department of Commerce (Commerce) also kicked off its leading role in the government-wide effort by **establishing** the U.S. Artificial Intelligence Safety Institute (USAISI), which will be led by the National Institute of Standards and Technology (NIST) and will spearhead efforts on AI safety and trust, particularly for the most advanced models.

In the ensuing months, federal agencies will continue to implement the EO’s over 90 initiatives to govern the development and use of AI. Below, please find a timeline outlining key directives in the EO and their accompanying deadlines.

The Akin cross-practice AI team continues to advise clients on navigating the evolving AI regulatory landscape and will closely track implementation of the EO’s directives and the resulting opportunities for industry engagement.

30 Days (November 29, 2023)	
General Services Administration (GSA)	Technology Modernization Fund: The Technology Modernization Board must consider prioritizing funding for AI projects, particularly generative AI, for the Technology Modernization Fund (TMF) for at least one year.
U.S. Department of Transportation (DOT)	AI in Transportation: Direct the Nontraditional and Emerging Transportation Technology (NETT) Council to examine the need for guidance regarding the use of AI in transportation.
45 Days (December 14, 2023)	
U.S. Department of Labor (DOL)	Attracting AI Talent: Solicit information from the private sector on where immigrants with advanced skills in science and technology are most needed.
Executive Office of the President (EOP)	Priority Mission Areas: The Office of Science and Technology Policy (OSTP) and OMB are directed to identify priority mission areas for increased government AI talent.

	Talent Task Force: The Assistant to the President and Deputy Chief of Staff for Policy must convene an AI and Technology Talent Task Force to further the hiring of AI and AI-enabling talent across the federal government.
60 Days (December 29, 2023)	
The Office of Personnel Management (OPM)	Hiring/Workplace Flexibility: Conduct an evidence-based review on the need for hiring and workplace flexibility.
EOP	Interagency Council: OMB is directed to convene and chair an interagency council to coordinate the development and use of AI in agencies’ programs and operations. The council must include key agency heads, the Director of National Intelligence and other agencies as identified by the chair.
90 Days (January 28, 2024)	
Commerce	<p>Dual-Use Foundation Models: Impose reporting obligations on companies developing or intending to develop potential “dual-use foundation models,” which are defined to include “an AI model that is trained on broad data, generally uses self-supervision, contains at least tens of billions of parameters, is applicable across a wide range of contexts and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters.” Specifically, such companies must report on (1) activities related to training, developing or producing dual-use foundation models; (2) the ownership and possession of the model weights of any dual-use foundation models and the measures taken to protect them; and (3) the results of any developed dual-use foundation model’s performance in relevant AI red-team testing guidance developed by NIST and related safety measures the company has taken.</p> <p>Until the Secretary of Commerce develops alternative criteria, this reporting requirement will apply to “any model that was trained using a quantity of computing power greater than 10²⁶ integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 10²³ integer or floating-point operations[.]”</p> <p>Large-Scale Computing Clusters: Require companies, individuals or other entities that acquire, develop or possess a potential large-scale computing cluster to report on certain factors, including the existence and location of these clusters and the amount of total computing power available in each.</p> <p>Until the Secretary of Commerce develops alternative criteria, this reporting requirement will apply to “any computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum computing capacity of 10²⁰ integer or floating-point operations per second for training AI.”</p> <p>IaaS Providers: Propose regulations that require U.S. Infrastructure as a Service (IaaS) providers to report foreign persons transacting on U.S. cloud to train large AI models that could be used for malicious cyber-related activities (training run). The</p>

	rules must also bar U.S. IaaS providers from providing such products unless the foreign reseller submits to the provider a report detailing each instance in which a foreign person transacts with the foreign reseller to use the U.S. IaaS product to conduct a training run.
U.S. Department of Homeland Security (DHS)	Critical Infrastructure Risks: The head of each agency with relevant regulatory authority over critical infrastructure and the heads of relevant sector risk management agencies (SRMAs), must provide to DHS an assessment of potential risks related to the use of AI in critical-infrastructure sectors.
U.S. Department of State	Attracting AI Talent: Alongside DHS, streamline visa applications and appointments for immigrants who plan to work on AI or other critical technologies.
OPM	Attracting AI Talent: Coordinate a pooled-hiring action informed by subject-matter experts and using skills-based assessments to support the recruitment of AI talent across agencies.
U.S. Department of Justice (DOJ)	Discriminatory Uses/Effects: The Civil Rights Division must convene the heads of federal civil rights offices to discuss their efforts to prevent discrimination in the use of automated systems and increase collaboration.
U.S. Department of Health and Human Services (HHS)	AI Task Force: Create an HHS AI Task Force that must, within 365 days, develop a plan for responsible deployment and use of AI and AI-enabled technologies (see prior alert outlining key health care takeaways here).
National Science Foundation (NSF)	National AI Research Resource Pilot: Launch a pilot program implementing the National AI Research Resource (NAIRR), consistent with past recommendations of the NAIRR Task Force. NSF must identify computational, data, software and training resources appropriate for inclusion in the NAIRR pilot.
GSA	FedRAMP: Develop and issue a framework for prioritizing critical and emerging technologies offerings in the Federal Risk and Authorization Management Program (FedRAMP) authorization process, which would apply for at least two years.
DOT	Recommendations on AI in Transportation: Direct appropriate Federal Advisory Committees to provide recommendations on the safe use of AI in transportation.
120 Days (February 27, 2024)	
DHS	Attracting AI Talent: Publish informational resources to better attract and retain experts in AI and other critical technologies.
U.S. Department of Defense (DoD)	Chemical, Biological, Radiological and Nuclear (CBRN) Threats: Enter into a contract with the National Academies of Sciences, Engineering and Medicine to conduct a study examining concerns and opportunities at the intersection of AI and synthetic biology.

U.S. Department of Energy (DOE)	High-Performance/Data-Intensive Computing: Consistent with available appropriations, establish a pilot program to enhance training programs for scientists, with the goal of training 500 new researchers by 2025.
U.S. Department of State	Attracting AI Talent: Consider initiating a rulemaking to establish new criteria to designate countries and skills on the Exchange Visitor Skills List as it relates to the two-year foreign residence requirement for certain J-1 nonimmigrants. Consider implementing a domestic visa renewal program to highly skilled talent in emerging technologies, as well as a program to identify and attract top talent at universities, research institutions and the private sector overseas.
U.S. Patent and Trademark Office (USPTO)	Inventorship of Patentable Subject Matter: Publish guidance for both patent examiners and applicants on how to address the use of AI.
OPM	Federal Hiring Practices: Issue guidance on existing pay flexibilities or incentive pay programs for AI, AI-enabling, and other key technical positions.
NSF	Privacy Research: Fund the creation of a Research Coordination Network (RCN) to further privacy research.
150 Days (March 28, 2024)	
U.S. Department of the Treasury (Treasury)	Best Practices for Financial Institutions: Submit a public report on best practices for financial institutions to manage AI-specific cybersecurity risks.
EOP	Agency Guidance: OMB is directed to issue guidance to agencies to strengthen the effective and appropriate use of AI. Within 60 days of the issuance of the guidance, OMB must develop a mechanism for federal agencies to assess their ability to adopt AI into their programs. Within 90 days of the issuance of the guidance, Commerce must develop practices to support implementation of the minimum risk-management practices. Within 180 days of the issuance of the guidance, OMB must develop a mechanism to ensure that agency contracts for the acquisition of AI systems are aligned.
NSF	Regional Innovation Engine: Fund and launch at least one NSF Regional Innovation Engine that prioritizes AI work.
180 Days (April 27, 2024)	
Commerce	CBRN Threats: Through NIST, initiate an effort to engage with industry and relevant stakeholders to develop and refine for possible use by synthetic nucleic acid sequence providers (1) specifications for effective nucleic acid synthesis procurement screening; (2) best practices, including security and access controls, for managing sequence-of-concern databases to support such screening; (3) technical

	<p>implementation guides for effective screening; and (4) conformity-assessment best practices and mechanisms.</p> <p>IaaS Reseller KYC: “Propose regulations that require United States IaaS Providers to ensure that foreign resellers of United States IaaS Products verify the identity of any foreign person that obtains an IaaS account . . . from the foreign reseller.”</p>
DHS	<p>Attracting AI Talent: Initiate policy changes to clarify and modernize immigration pathways for experts in AI and other critical and emerging technologies and consider beginning a rulemaking to modernize the H-1B program.</p> <p>AI Risk Management Framework: Incorporate the AI Risk Management Framework, NIST AI 100-1, as well as other appropriate security guidance, into safety and security guidelines for use by critical infrastructure owners and operators. DHS would then coordinate with agency heads to take steps for the federal government to mandate such guidelines.</p> <p>Cyber Defenses: Complete an operational pilot project test, evaluate, and deploy AI capabilities to help remediate vulnerabilities in critical U.S. government software, systems, and networks.</p> <p>CBRN Threats: Evaluate the potential for AI to be misused to enable the development or production of CBRN threats and develop a framework to conduct structured evaluation and stress testing of nucleic acid synthesis procurement screening.</p> <p>Intellectual Property Risks: Develop a program to help developers mitigate AI-related intellectual property (IP) risks.</p>
DoD	<p>Cyber Defenses: Complete an operational pilot project to test, evaluate and deploy AI capabilities, such as large-language models, to aid in the discovery and remediation of vulnerabilities in critical U.S. government software, systems and networks.</p> <p>Attracting AI Talent: Submit a report to the White House outlining recommendations to address gaps in AI talent for national defense.</p>
DOE	<p>AI in Energy: Among other things, establish an office to coordinate development of AI and other emerging technologies across DOE programs and the National Laboratories.</p>
DOL	<p>Employer Guidance: Publish best practices for employers that could be used to mitigate AI’s potential harms to employees’ wellbeing. Agency heads must consider encouraging the adoption of such best practices.</p> <p>Worker Displacement: Submit to the President a report analyzing the abilities of federal agencies to support workers displaced by the adoption of AI.</p>
OPM	<p>Generative AI Guidance: Develop guidelines on the use of generative AI by the federal workforce.</p> <p>Government-Wide Hiring Guidance: Establish guidance and policy on government-wide hiring of AI, data and technology talent. Establish an interagency working group to facilitate hiring of people with AI and other technical skills. Review competencies</p>

	for civil engineers and other related positions and make recommendations for ensuring AI expertise and credentials in such positions.
EOP	<p>CBRN Threats: OSTP is directed to establish a framework, incorporating existing guidance, to encourage providers of synthetic nucleic acid sequences to implement comprehensive procurement screening mechanisms.</p> <p>Scientific Research: The President’s Council of Advisors on Science and Technology (PCAST) is directed to publish a report on the potential role of AI and issues that may hinder the effective use of the technology in research.</p>
DOJ	Recruitment/Training of Law Enforcement: The interagency working group must identify and share best practices for recruiting and hiring of law enforcement professionals with relevant technical skills and training law enforcement professionals about responsible application of AI.
HHS	<p>Public Benefits/Services: Publish a plan on the use of automated or algorithmic systems in the implementation by States and localities of public benefits and services.</p> <p>Responsible Health Care Deployment Strategy: Direct HHS offices to develop a strategy to determine whether AI-enabled technologies in the health care space maintain appropriate levels of quality.</p> <p>Providers’ Compliance with Nondiscrimination Laws: Consider ways advance compliance with federal nondiscrimination laws by HHS providers that receive federal funding.</p>
GSA	Acquisition Solutions: Work to facilitate access to acquisition solutions for certain types of AI services and products.
U.S. Department of Housing and Urban Development (HUD)	Fair-Lending/Housing: Alongside the Consumer Financial Protection Bureau (CFPB), issue guidance on how fair-lending and housing laws will prevent discrimination by AI in digital advertisements for credit and housing, as well as guidance on the use of tenant screening systems.
DOT	Prioritization of Grants: Direct the Advanced Research Projects Agency-Infrastructure (ARPA-I) to examine the challenges and opportunities of AI and prioritize the allocation of grants to those opportunities.
U.S. Department of Agriculture (USDA)	Benefit Programs: Issue guidance to State, local, Tribal and territorial public-benefits administrators on the use of automated or algorithmic systems in implementing benefits or providing customer support for such programs.
240 Days (June 26, 2024)	
Commerce	Content Authentication: Provide a report to the Office of Management and Budget (OMB) and the White House identifying practices for authenticating content and tracking its provenance; labeling and detecting synthetic content; preventing generative AI from producing Child Sexual Abuse Material (CSAM), among other

	<p>things. Within 180 days of the report, develop guidance regarding the existing tools and practices for digital content authentication and synthetic content detection measures. OMB must then issue guidance to agencies for labeling and authenticating official U.S. government digital content that they produce or publish. The Federal Acquisition Regulatory Council is also directed to consider amending the Federal Acquisition Regulation (FAR) to reflect the guidance.</p> <p>NIST Best Practices: Through NIST, develop best practices for deploying safe and trustworthy AI systems, including by developing companion resource to the AI Risk Management Framework for generative AI, developing a secure software development framework for generative AI and for dual-use foundation models and creating guidance for evaluating and auditing AI capabilities.</p> <p>Dual-Use Foundation Models: Through NIST, establish guidelines to enable developers of AI, particularly of dual-use foundation models, to conduct AI red-teaming tests. Solicit stakeholder input on potential risks and benefits of dual-use foundation models and submit a report to the President with related recommendations.</p> <p>Global Standards: Establish a plan for global engagement on promoting and developing AI standards. Within 180 days of establishing the plan, Commerce must submit a report to the President with related recommendations.</p>
NSF	<p>Privacy-Enhancing Technologies (PETs): Coordinate with federal agencies on potential opportunities to leverage PETs.</p>
270 Days (July 26, 2024)	
DHS	<p>Cross-Border/Global Risks: Develop a plan for multilateral engagements to further the adoption of the newly developed AI safety and security guidelines for critical infrastructure owners and operators. Within 180 days of establishing the plan, DHS must submit a report to the President on needed actions to reduce cross-border risks to critical U.S. infrastructure.</p> <p>Safety and Security Advisory Committee: Establish an Artificial Intelligence Safety and Security Advisory Committee, to be comprised of AI experts from the private sector, academia and government.</p> <p>International Collaboration: Lead collaboration with international partners to mitigate the risk of critical infrastructure disruptions resulting from incorporation of AI into critical infrastructure systems or malicious use of AI.</p>
DOE	<p>AI Model Evaluation Tools: Develop and, to the extent possible by available appropriations, implement a plan for developing DOE’s AI model evaluation tools and AI testbeds.</p>
USPTO	<p>AI/IP Guidance: Issue additional guidance to patent examiners and applicants to address other issues at the intersection of AI and IP.</p> <p>Consult with the U.S. Copyright Office and issue recommendations to the President on potential executive actions at the intersection of copyright and AI.</p>

U.S. Copyright Office	Copyright Protections: Recommend additional executive actions the White House can take to address issues related to copyright protections for AI-generated work and the use of copyrighted work to train AI algorithms (or 180 days after the Copyright Office publishes its AI study, whichever is later).
EOP	National Security Memorandum: Oversee an interagency process of developing and submit to the President a National Security Memorandum on AI, which will, among other things, outline actions for federal agencies to address the national security risks and potential benefits posed by AI.
DOJ	Attorney General Recruitment Recommendations: The Attorney General must consider best practices developed by the interagency working group for recruiting and hiring of law enforcement professionals with relevant technical skills and, if needed, develop additional recommendations for State, local, Tribal and territorial law enforcement agencies and criminal justice agencies.
365 Days (October 29, 2024)	
Commerce	PETs: Create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI.
U.S. Department of State	Global Development: Publish an AI in Global Development Playbook that incorporates the AI Risk Management Framework’s guidelines, as well as develop a Global AI Research Agenda.
DOL	Nondiscrimination Guidance for Contractors: Publish guidance for federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems.
OPM	Attracting AI Talent: Implement new Executive Core Qualifications (ECQs) in the Senior Executive Service (SES) assessment process.
DOJ	Criminal Justice System: Submit to the President a report that addresses the use of AI in the criminal justice system. If needed, reassess the existing capacity to investigate law enforcement deprivation of rights resulting from the use of AI.
HHS	<p>Responsible AI Task Force: Create a task force to develop a strategic plan on the responsible use of AI, including with respect to generative AI.</p> <p>AI Safety Program: Establish an AI safety program that, in partnership with voluntary federally listed Patient Safety Organizations establishes a framework for approaches to identifying and capturing clinical errors resulting from AI deployed in health care settings, among other things.</p> <p>AI in Drug-Development Processes: Develop a strategy for regulating the use of AI or AI-enabled tools in drug-development processes.</p>
U.S. Department of Education	AI in Education: Develop guidance on ensuring responsible and nondiscriminatory uses of AI in education.

U.S. Department of Veterans Affairs (VA)	Tech Sprint Competitions: Host two three-month nationwide AI Tech Sprint competitions. On October 31, 2023, the VA formally launched the challenge, which will remain open until January 5, 2024.
540 Days (April 22, 2025)	
NSF	National AI Research Institutes: Establish at least four new National AI Research Institutes.

If you have questions about this client alert, please contact any Akin lawyer or advisor below:

Shiva Aminian
saminian@akingump.com
+1 310.552.6476

Jingli Jiang
jjiang@akingump.com
+1 202.887.4250

Natasha Kohne
nkohne@akingump.com
+1 415.765.9505

Susan Lent
slent@akingump.com
+1 202.887.4558

Ed Pagano
epagano@akingump.com
+1 202.887.4255

Michelle Reed
mreed@akingump.com
+1 214.969.2713

Hans Rickhoff
hrickhoff@akingump.com
+1 202.887.4145

David Vondle
dvondle@akingump.com
+1 202.887.4184

Reggie Babin
rbabin@akingump.com
+1 202.887.4140

Casey Higgins
cchiggins@akingump.com
+1 202.887.4223

Ryan Thompson
thompsonr@akingump.com
+1 202.887.4138

Alan Hayes
amhayes@akingump.com
+1 202.887.4272

Maka Hutson
mhutson@akingump.com
+1 214.969.2781

Thomas Krueger
tkrueger@akingump.com
+1 202.887.4215

Taylor Daly
tdaly@akingump.com
+1 202.416.5541