

THE WHITE HOUSE



[Administration](#) [The Record](#) [Briefing Room](#) [Visit](#)

OCTOBER 30, 2023

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

---

 [BRIEFING ROOM](#) [PRESIDENTIAL ACTIONS](#)

---

# President Biden issued an Executive Order to “ensure that America leads the way in seizing the promise and managing the risks of AI”



# Sections in the EO

1. Purpose
2. Policy and Principles
3. Definitions
4. Ensuring the Safety and Security of AI Technology
5. Promoting Innovation and Competition
6. Supporting Workers
7. Advancing Equity and Civil Rights
8. Protecting Consumers, Patients, Passengers, and Students
9. Protecting Privacy
10. Advancing Federal Government Use of AI
11. Strengthening American Leadership Abroad
12. Implementation
13. General Provisions

# Sections in the EO

1. Purpose
2. Policy and Principles
3. Definitions
4. Ensuring the Safety and Security of AI Technology
5. Promoting Innovation and Competition
6. Supporting Workers
7. Advancing Equity and Civil Rights
8. Protecting Consumers, Patients, Passengers, and Students
9. Protecting Privacy
10. Advancing Federal Government Use of AI
11. Strengthening American Leadership Abroad
12. Implementation
13. General Provisions

**Key AI actions following  
the executive order**

## **Discussion points**

1. Definitions
2. Red teaming
3. Innovation & regulation
4. Supporting workers
5. Trump administration
6. Concluding discussion points

~70 pages... most of it contains actions/deadlines that federal government agencies should take to meet the priorities listed in the executive order

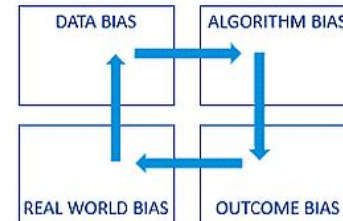
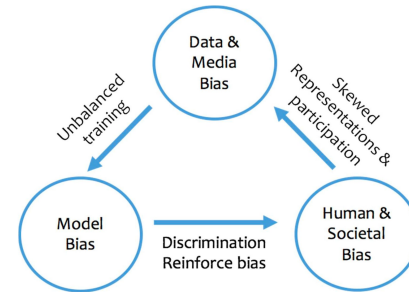
# Purpose: Harnessing AI for good and realizing its benefits requires mitigating its substantial risks

**“My Administration places the highest urgency on governing the development and use of AI safely and responsibly, and is therefore advancing a coordinated, Federal Government-wide approach to doing so.”**

**Responsible AI** = solve urgent challenges while making world more prosperous, productive, innovative, secure

**Irresponsible AI** = exacerbate societal harms (fraud, discrimination, bias, disinformation), displace and disempower workers, competition, national security risks

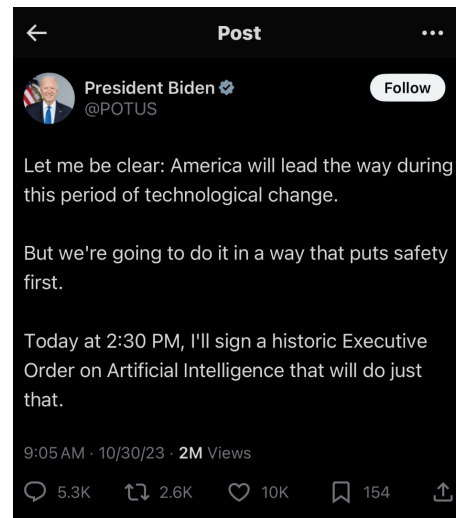
*“In the end, AI reflects the principles of the people who build it, the people who use it, and the data upon which it is built.”*



# Policy and Principles

Lays out 8 guiding principles for federal agencies to follow

1. AI must be safe and secure
2. Innovation, competition, and collaboration
3. Commitment to supporting American workers
4. AI must advance equity and civil rights
5. American consumers must be protected
6. Americans' privacy and civil liberties must be protected as AI continues advancing
7. Increase Federal Government's capacity to regulate, govern, & support responsible AI
8. Federal government should lead the way to global societal, economic, and technological progress



# Definitions

1. Agency
2. Artificial Intelligence (AI)
3. AI Model
4. AI Red-Teaming
5. AI System
6. Commercially Available Information
7. Crime Forecasting
8. Critical and Emerging Technologies
9. Critical Infrastructure
10. Differential-Privacy Guarantee
11. Dual-Use Foundation Model
12. Federal Law Enforcement Agency
13. Floating-Point Operation
14. Foreign Person
15. Foreign Reseller
16. Generative AI
17. Infrastructure as a Service (IaaS)
18. Integer Operation
19. Intelligence Community
20. Machine Learning
21. Model Weight
22. National Security System
23. Omics
24. Open RAN
25. Personally Identifiable Information (PII)
26. Privacy-Enhancing Technology (PET)
27. Privacy Impact Assessment
28. Sector Risk Management Agency
29. Self-Healing Network
30. Synthetic Biology
31. Synthetic Content
32. Testbed
33. Watermarking

# Definitions

**“AI red-teaming”** means a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. Artificial Intelligence red-teaming is most often performed by dedicated “red teams” that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.

**“generative AI”** means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

**“privacy-enhancing technology”** means any software or hardware solution, technical process, technique, or other technological means of mitigating privacy risks arising from data processing, including by enhancing predictability, manageability, disassociability, storage, security, and confidentiality. These technological means may include secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic-data-generation tools.

**“floating-point operation”** means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base.

**“dual-use foundation model”** means 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, such as by:

- (i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;
- (ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks;
- or (iii) permitting the evasion of human control or oversight through means of deception or obfuscation.



# Discussion

Are there any terms you think should have been included or defined differently? How do the definitions affect governance efforts? Who should be defining these terms?

1. Agency
2. Artificial Intelligence (AI)
3. AI Model
4. AI Red-Teaming
5. AI System
6. Commercially Available Information
7. Crime Forecasting
8. Critical and Emerging Technologies
9. Critical Infrastructure
10. Differential-Privacy Guarantee
11. Dual-Use Foundation Model
12. Federal Law Enforcement Agency
13. Floating-Point Operation
14. Foreign Person
15. Foreign Reseller
16. Generative AI
17. Infrastructure as a Service (IaaS)
18. Integer Operation
19. intelligence Community
20. Machine Learning
21. Model Weight
22. National Security System
23. Omics
24. Open RAN
25. Personally Identifiable Information (PII)
26. Privacy-Enhancing Technology (PET)
27. Privacy Impact Assessment
28. Sector Risk Management Agency
29. Self-Healing Network
30. Synthetic Biology
31. Synthetic Content
32. Testbed
33. Watermarking

# New standards for AI Safety and Security

## Require that developers of the most powerful AI systems share their safety test results and other critical information with the U.S. government

*“In accordance with the Defense Production Act, the Order will require that **companies developing any foundation model that poses a serious risk to national security, national economic security, or national public health and safety must notify the federal government when training the model, and must share the results of all red-team safety tests.** These measures will ensure AI systems are safe, secure, and trustworthy before companies make them public.”*

## Develop standards, tools, and tests to help ensure that AI systems are safe, secure, and trustworthy

*“The **National Institute of Standards and Technology will set the rigorous standards for extensive red-team testing to ensure safety before public release.** The Department of Homeland Security will apply those standards to critical infrastructure sectors and establish the AI Safety and Security Board. The Departments of Energy and Homeland Security will also address AI systems’ threats to critical infrastructure, as well as chemical, biological, radiological, nuclear, and cybersecurity risks. Together, these are the most significant actions ever taken by any government to advance the field of AI safety.”*

# Red teaming discussion

**“AI red-teaming”** means a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. Artificial Intelligence red-teaming is most often performed by dedicated “red teams” that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.

**Are there other ways to audit models besides AI red-teaming. How do we ensure that AI red-teaming is done in a comprehensive manner?**

**– Nandeeka**

## Some other things that can be discussed wrt red teaming

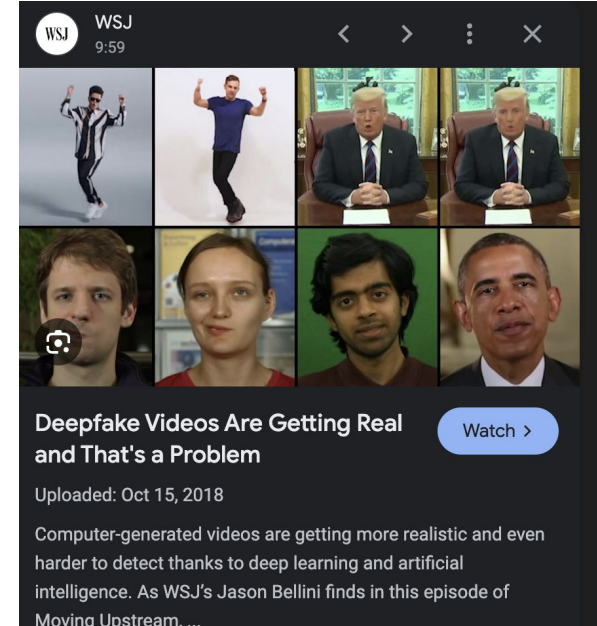
1. What types of *undesirable behaviors, limitations, and risks* can or should be effectively caught and mitigated through red-teaming exercises?
2. aside from AI developers, who else should be at the table, and what resources should be available to them?
3. How should the risks identified through red-teaming be *documented, reported, and managed*?
4. Is red-teaming on its own sufficient for assessing and managing the safety, security, and trustworthiness of AI? If not, what other practices should be part of the broader evaluation toolbox, and how does red-teaming complement those approaches?

Protect against the risks of using AI to engineer dangerous biological materials

# New standards for AI Safety and Security: Watermarking

**Protect Americans from AI-enabled fraud and deception by establishing standards and best practices for detecting AI-generated content and authenticating official content**

*“The Department of Commerce will develop guidance for content authentication and watermarking to clearly label AI-generated content. Federal agencies will use these tools to **make it easy for Americans to know that the communications they receive from their government are authentic**—and set an example for the private sector and governments around the world.”*



# New standards for AI Safety and Security:

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 regarding the following:

- (A) **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;
- (B) **the ownership and possession of the model weights of any dual-use foundation models**, and the physical and cybersecurity measures taken to protect those model weights; and
- (C) **the results of any developed dual-use foundation model's performance in relevant AI red-team testing** based on guidance developed by NIST

# New standards for AI Safety and Security:

Companies, individuals, or other organizations or entities that acquire, develop, or possess a potential large-scale computing cluster to report any such acquisition, development, or possession, including the existence and location of these clusters and the amount of total computing power available in each cluster.

**any model that was trained using a quantity of computing power greater than  $10^{26}$  integer floating-point operations**, or using primarily biological sequence data and using a quantity of computing power greater than  $10^{23}$  integer or floating-point operations; and

**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  $10^{20}$  integer or floating-point operations per second for training AI

## 2.3 A MISPLACED FOCUS ON FLOPS

**FLOPs.** Floating point operations. The cumulative number of floating point operations (e.g., 3.5 x 7.1) used during model training. Not to be confused with floating point operations *per second* (FLOPS, with a capital S).

Definitions of foundation and frontier models (see Table 1) include regulatory thresholds defined by cumulative training FLOPs. These numbers have no basis in outcomes or technical reality, as we demonstrate in the following section.  $10^{26}$  FLOPs appeared as an arbitrary FLOPs threshold in the October 2023 Biden Administration Executive Order.

# Promoting innovation and competition

Encourages innovation through:

- Streamlined visa and immigration processes for AI talent
- **Promote a fair, open, and competitive AI ecosystem**

*by providing small developers and entrepreneurs access to technical assistance and resources, helping small businesses commercialize AI breakthroughs, and encouraging the Federal Trade Commission to exercise its authorities*

- Expanding AI research funding (through the National AI Research Resource—a trust that will provide AI researchers and students to key AI resources and data)



[Home](#) / [Our Focus Areas](#) / [Artificial Intelligence](#) / [National Artificial Intelligence Research Resource Pilot](#)

## About the NAIRR pilot

The NAIRR is a concept for a national infrastructure that connects U.S. researchers to computational, data, software, model and training resources they need to participate in AI research.

The NAIRR pilot, as directed in the [Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence](#), is a proof-of-concept for the eventual full-scale NAIRR. The pilot will focus on supporting research and education across the nationwide research community, while gaining insights that will refine the design of a full NAIRR.

The NAIRR pilot will run for two years, beginning January 24, 2024. The pilot will broadly support fundamental, translational and use-inspired AI-related research with particular emphasis on societal challenges. Initial priority topics include safe, secure and trustworthy AI; human health; and environment and infrastructure. A broader array of priority areas will be supported as the pilot progresses. The pilot will also support educators to train students on responsible use and development of AI technologies by providing access to infrastructure and training resources.

NAIRR is a vision of a national infrastructure for AI research and discovery

enabling and user-friendly access to the NAIRR vision

connecting other federal agencies and government departments to the NAIRR vision and research and



- About
- How
- NAIRR
- About
- Add



# Discussion on innovation

## *Balancing innovation and regulation?*

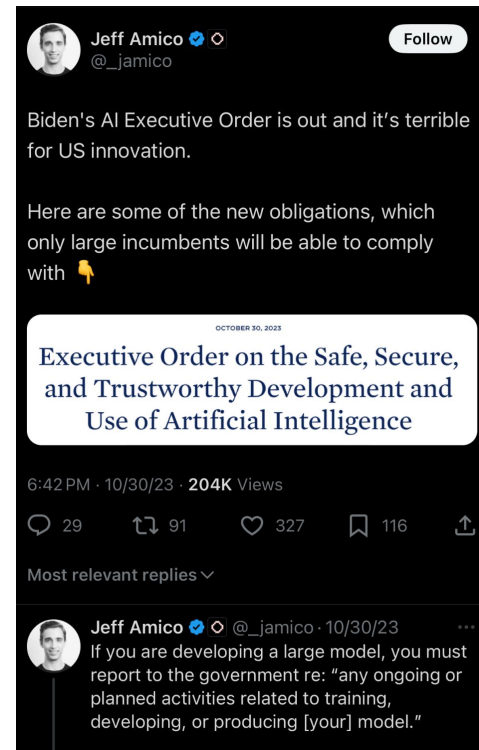
How can the government implement testing requirements without stifling innovation or creating excessive regulatory burden for smaller AI companies and startups? – **Anish**

There is a valid concern that an attempt to regulate AI may not empower research to get more cutting edge results, how will we be competing with near peer adversary countries when the sky may be the limit in their AI development paradigm. – **Jerome**

How can the Federal Government effectively balance the promotion of AI innovation and competition while ensuring the safety and reliability of AI systems, in order to prevent overregulation that may stifle technological advancement and to foster a diverse and inclusive AI ecosystem? – **Junyi**



A screenshot of a tweet from Sam Altman (@sama) on X. The tweet text reads: "there are some great parts about the AI EO, but as the govt implements it, it will be important not to slow down innovation by smaller companies/ research teams." Below the text, it says "i am pro-regulation on frontier systems, which is what openai has been calling for, and against regulatory capture." The tweet is dated 12:45 PM · 11/2/23 and has 689K views. It shows 301 replies, 282 retweets, 2.4K likes, and 210 bookmarks. A reply from Sam Altman is visible, dated 11/2/23, with the text: "(there is nuance in saying 'regulate us, but not smaller competitors' that somehow ends up getting lost and we just get bashed, but i think it's important enough to be worth it.)" The reply has 62 replies, 53 retweets, 567 likes, and 254K views.



A screenshot of a tweet from Jeff Amico (@\_jamico) on X. The tweet text reads: "Biden's AI Executive Order is out and it's terrible for US innovation." Below the text, it says "Here are some of the new obligations, which only large incumbents will be able to comply with 🗡️". The tweet is dated 6:42 PM · 10/30/23 and has 204K views. It shows 29 replies, 91 retweets, 327 likes, and 116 bookmarks. A reply from Jeff Amico is visible, dated 10/30/23, with the text: "If you are developing a large model, you must report to the government re: 'any ongoing or planned activities related to training, developing, or producing [your] model.'" The reply has 116 replies, 91 retweets, 327 likes, and 116 bookmarks. A white box highlights the title of the Executive Order: "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence".

# Protecting Americans' Privacy

- Protect Americans' privacy by prioritizing federal support for accelerating the development and use of privacy-preserving techniques
- Strengthen privacy-preserving research and technologies
- Evaluate how agencies collect and use commercially available information

# Advancing Equity and Civil Rights

To ensure that AI advances equity and civil rights, the President directs the following additional actions:

- Provide clear guidance to landlords, Federal benefits programs, and federal contractors to keep AI algorithms from being used to exacerbate discrimination.
- Address algorithmic discrimination through training, technical assistance, and coordination between the Department of Justice and Federal civil rights offices on best practices for investigating and prosecuting civil rights violations related to AI.
- Ensure fairness throughout the criminal justice system by developing best practices on the use of AI in sentencing, parole and probation, pretrial release and detention, risk assessments, surveillance, crime forecasting and predictive policing, and forensic analysis.



# Advancing Equity and Civil Rights

*“Irresponsible uses of AI can lead to and deepen discrimination, bias, and other abuses in justice, healthcare, and housing. The Biden-Harris Administration has already taken action by publishing the [Blueprint for an AI Bill of Rights](#) and issuing an [Executive Order directing agencies to combat algorithmic discrimination](#), while enforcing existing authorities to protect people’s rights and safety.”*



# BLUEPRINT FOR AN AI BILL OF RIGHTS

MAKING AUTOMATED SYSTEMS WORK FOR  
THE AMERICAN PEOPLE

*“Irresponsible uses of AI can lead to and deepen discrimination, bias, and other abuses in justice, healthcare, and housing. The Biden-Harris Administration has already taken action by publishing the [Blueprint for an AI Bill of Rights](#) and issuing an [Executive Order](#) directing agencies to combat algorithmic discrimination, while enforcing existing authorities to protect people’s rights and safety.”*



[Safe and Effective  
Systems](#)



[Algorithmic  
Discrimination  
Protections](#)



[Data Privacy](#)



[Notice and  
Explanation](#)

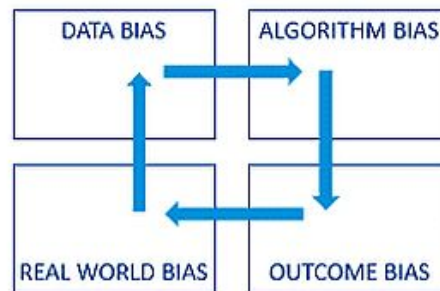


[Human  
Alternatives,  
Consideration, and  
Fallback](#)

# Advancing Equity and Civil Rights

Focuses on addressing algorithmic discrimination:

- Provide clear guidance to landlords, Federal benefits programs, and federal contractors to keep AI algorithms from being used to exacerbate discrimination
- Promoting fairness in hiring, housing, and access to services
- Fairness in criminal justice (sentencing, parole, probation, etc)



# Standing Up for Consumers, Patients, and Students

To protect consumers while ensuring that AI can make Americans better off, the President directs the following actions:

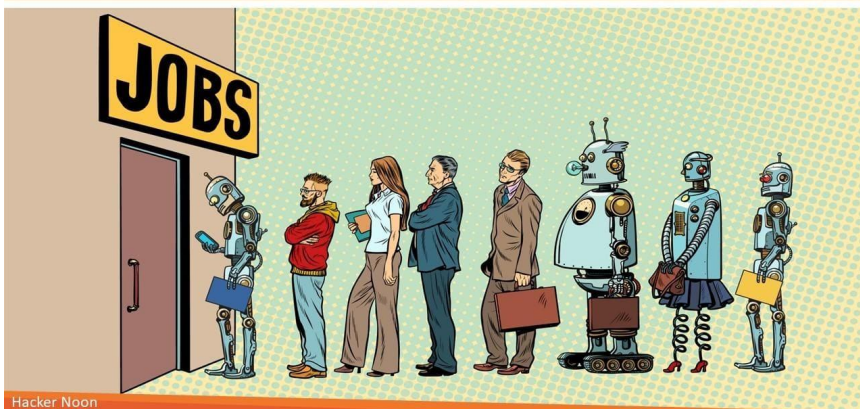
- Advance the responsible use of AI in healthcare and the development of affordable and life-saving drugs.
- Shape AI's potential to transform education by creating resources to support educators deploying AI-enabled educational tools, such as personalized tutoring in schools.

# Supporting Workers

**AI is changing America's jobs and workplaces, offering both the promise of improved productivity but also the dangers of increased workplace surveillance, bias, and job displacement**

- Develop principles and best practices to mitigate the harms and maximize the benefits of AI for workers by addressing job displacement; labor standards; workplace equity, health, and safety
- Produce a report on AI's potential labor-market impacts, and study and identify options for strengthening federal support for workers facing labor disruptions, including from AI

**Some Professions will Fall in Decay, Others will Thrive, and Most of Them will Drastically Change**

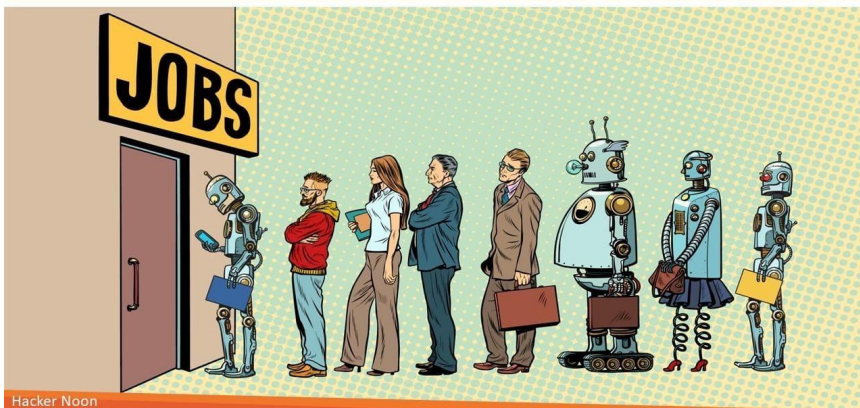




# Supporting Workers

“My Administration will seek to **adapt job training** and education to support a diverse workforce and help provide access to opportunities that AI creates. In the workplace itself, **AI should not be deployed in ways that undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or cause harmful labor-force disruptions.**”

**Some Professions will Fall in Decay, Others will Thrive, and Most of Them will Drastically Change**



## Question

I feel that there isn't much said about preventing the displacement of jobs - perhaps there is no good sense of how to help workers at risk of their jobs being automated, especially for labor-intensive ones like manufacturing warehouses whose AI counterparts are already showing signs of matching their capabilities. Additionally, AI was meant to wash our dishes and fold our laundry, and yet it came directly at our creative jobs in the last few years. How can we revert back to a point in which they carry out our labor while letting us enjoy our creative endeavors?

– Ryan

## Advancing American Leadership Abroad


AI's challenges and opportunities are global. The Biden-Harris Administration will continue working with other nations to support safe, secure, and trustworthy deployment and use of AI worldwide. To that end, the President directs the following actions:

- Expand bilateral, multilateral, and multistakeholder engagements to collaborate on AI. The State Department, in collaboration, with the Commerce Department will lead an effort to establish robust international frameworks for harnessing AI's benefits and managing its risks and ensuring safety.
- Promote the safe, responsible, and rights-affirming development and deployment of AI abroad to solve global challenges, such as advancing sustainable development and mitigating dangers to critical infrastructure.
-


# Ensuring Responsible and Effective Government Use of AI

To ensure the responsible government deployment of AI and modernize federal AI infrastructure, the President directs the following actions:

- Issue guidance for agencies' use of AI,
- Help agencies acquire specified AI products and services faster, more cheaply, and more effectively through more rapid and efficient contracting.
- Accelerate the rapid hiring of AI professionals as part of a government-wide AI talent surge led by the Office of Personnel Management, U.S. Digital Service, U.S. Digital Corps, and Presidential Innovation Fellowship. Agencies will provide AI training for employees at all levels in relevant fields.

 **Arvind Narayanan** ✓  
@random\_walker

My meta-takeaway from the full text of the Executive Order on AI is that in the next 6-12 months there will be an unfathomable number of guidelines, rulemaking processes, reports, whitepapers, working groups, public comments, panels, and whatnot.

 whitehouse.gov  
**Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**  
By the authority vested in me as President by the Constitution and the laws of the United States of America...

2:19 PM · Oct 30, 2023 · **71.7K** Views

21 67 314 74

 **François Chollet** ✓  
@fchollet

Biden's executive order on AI, on its own, is fairly innocuous. But its existence and contents are proof that the AI regulatory capture lobby is making fast progress towards its goal of completely locking down the space. Will likely happen within the next five years.

9:33 AM · Oct 31, 2023 · **195.6K** Views

38 115 623 66

3 months later...

JANUARY 29, 2024

# Fact Sheet: Biden-Harris Administration Announces Key AI Actions Following President Biden's Landmark Executive Order



▶ BRIEFING ROOM

▶ STATEMENTS AND RELEASES

# The table below summarizes many of the activities federal agencies have completed in response to the Executive Order

Action	Agency	Required Timeline
Evaluated ways to prioritize agencies' adoption of AI through the Technology Modernization Fund	Technology Modernization Board	30 days
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
Reported federal agency resources available to incorporate into the National AI Research Resource (NAIRR) pilot	Agencies identified by the National Science Foundation	45 days
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
Convened AI and Tech Talent Task Force	White House Chief of Staff's Office	45 days
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
Published a Request for Information (RFI) on whether to revise the list of Schedule A job classifications that do not require permanent labor certifications	Department of Labor	45 days
Convened an interagency council to coordinate federal agencies' use of AI	Office of Management and Budget	60 days
Reviewed the need for -- and granted -- flexible hiring authorities including direct hire and excepted service authorities for federal agencies to hire AI professionals	Office of Personnel Management	60 days
Used Defense Production Act authorities to compel developers of powerful AI systems to report vital information, especially AI safety test results	Department of Commerce	90 days
Proposed a draft rule that compels U.S. cloud companies that provide computing power for foreign AI training to report that they are doing so	Department of Commerce	90 days
Completed risk assessments covering AI's use in every critical infrastructure sector	Sector Risk Management Agencies	90 days

Launched a pilot of the NAIRR	National Science Foundation	90 days	COMPLETE
Streamlined visa processing, including by renewing and expanding interview-waiver authorities	Department of State	90 days	COMPLETE
Established an AI Task Force to develop policies to provide regulatory clarity and catalyze AI innovation in healthcare	Department of Health and Human Services	90 days	COMPLETE
Convened federal agencies' civil rights offices to discuss the intersection of AI and civil rights	Department of Justice	90 days	COMPLETE
Directed key Federal Advisory Committees to advise on AI and transportation	Department of Transportation	90 days	COMPLETE
Launched a pooled hiring action, to accelerate federal AI hiring, by letting certain applicants apply for roles in multiple agencies with just one application	Office of Personnel Management	90 days	COMPLETE
Released a draft framework for prioritizing generative AI technologies in security authorizations for federally procured products and services	General Services Administration	90 days	COMPLETE
Announced the funding of new Regional Innovation Engines (NSF Engines), including with a focus on advancing AI	National Science Foundation	150 days	COMPLETE
Released an RFI on how federal agencies' privacy impact assessments may be more effective at mitigating privacy risks, including those that are further exacerbated by AI and other advances in technology and data capabilities.	Office of Management and Budget	180 days	COMPLETE
Established an office to coordinate development of AI and other critical and emerging technologies across the agency	Department of Energy	180 days	COMPLETE
Released for comment a draft policy on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence	Office of Management and Budget	(none)	COMPLETE
Launched the EducateAI initiative, in order to prioritize AI-related workforce development	National Science Foundation	(none)	COMPLETE
Defined AI as a focus area for prize funds through the 2024 Growth Accelerator Fund Competition	Small Business Administration	(none)	COMPLETE
Confirmed the eligibility of AI-related expenditures for support via key programs that benefit small businesses	Small Business Administration	(none)	COMPLETE
Published an RFI on AI's implications for global development	U.S. Agency for International Development & Department of State	(none)	COMPLETE
Proposed changes to a privacy rule that would further limit companies' ability to monetize children's data, including by limiting targeted advertising	Federal Trade Commission	(none)	COMPLETE
Issued an advisory opinion to highlight that false, incomplete, and old information must not appear in background check reports, including for tenant screening	Consumer Financial Protection Bureau	(none)	COMPLETE

6 months later...

APRIL 29, 2024

# Biden-Harris Administration Announces Key AI Actions 180 Days Following President Biden's Landmark Executive Order



► BRIEFING ROOM

► STATEMENTS AND RELEASES

**“federal agencies reported that they completed all of the 180-day actions in the E.O. on schedule, following their recent successes completing each 90-day, 120-day, and 150-day action on time.”**

Published guidance on patentability of AI-assisted inventions	U.S. Patent and Trademark Office	120 days	COMPLETE	Dedicated personnel to collect, analyze, and investigate AI-enabled digital piracy and continued to investigate theft of AI IP and trade secrets, as well as insider threats	Department of Homeland Security	180 days	COMPLETE				
Launched a pilot program for a domestic visa renewals	Department of State	120 days	COMPLETE	Published a report on AI's potential to improve planning, permitting, investment, and operations for electric grid infrastructure and to enable clean power provision	Department of Energy	180 days	COMPLETE				
Entered into a contract with the National Academies of Sciences, Engineering, and Medicine to conduct a study regarding AI, biological data, and biosecurity risks	Department of Defense	120 days	COMPLETE	Developed AI tools -- and tools to facilitate building foundation models -- that can advance basic and applied science	Department of Energy	180 days	COMPLETE	Reviewed AI and data competencies for Executive Core Qualifications for Senior Executive Service roles	Office of Personnel Management	180 days	COMPLETE
Issued guidance on how federal agencies can use benefits, flexibilities, and incentives to attract, hire, and retain AI and AI-enabling talent	Office of Personnel Management	120 days	COMPLETE	Collaborated with private-sector actors to develop AI tools that can address climate change and other challenges	Department of Energy	180 days	COMPLETE	Reviewed AI competencies needed for civil engineers and other roles in the federal government	Office of Personnel Management	180 days	COMPLETE
Published information accessible on AI.gov to help experts in AI understand options for working in the United States	Department of Homeland Security	120 days	COMPLETE	Launched partnerships to expand the use of Department of Energy testbeds and computing capabilities for new applications in science, energy, and national security	Department of Energy	180 days	COMPLETE	Submitted a report with policy recommendations regarding the Department of Defense's hiring and employment of noncitizens, including ones with skills in AI and related fields	Department of Defense	180 days	COMPLETE
Published a report with data on how experts in AI and other critical and emerging technologies have utilized the immigration system	Department of Homeland Security	120 days	COMPLETE	Authored a report on AI's potential role to help tackle major societal challenges	President's Council of Advisors on Science and Technology	180 days	COMPLETE	Published a guide for federal contractors and subcontractors to answer questions and share promising practices to clarify federal contractors' legal obligations, promote equal employment opportunity, and mitigate the potentially harmful impacts of AI in employment decisions	Department of Labor	365 days	COMPLETE
Evaluated steps for updating -- and establishing new criteria for -- the countries and skills on the Exchange Visitor Skills List, including those skills critical to the United States	Department of State	120 days	COMPLETE	Submitted a report to the President on AI's labor-market effects	Council of Economic Advisors	180 days	COMPLETE	Published guidance regarding the application of the Fair Labor Standards Act and other federal labor standards as employers increasingly use AI and other automated technologies in the workplace	Department of Labor	(none)	COMPLETE
Published a final memorandum with requirements and guidance for federal agencies' AI governance, innovation, and risk management	Office of Management and Budget	150 days	COMPLETE	Submitted a report to the President evaluating policy options for supporting workers displaced by the adoption of AI and other technologies -- including assessments of current and former federal programs	Department of Labor	180 days	COMPLETE	Launched the AI Safety and Security Board to advise on safe and secure development and deployment of AI in critical infrastructure	Department of Homeland Security	(none)	COMPLETE
Published a report examining AI-related cybersecurity and fraud risks and best practices for financial institutions	Department of Treasury	150 days	COMPLETE	Developed principles and best practices for employers and developers to develop and deploy workplace uses of AI in ways that are safe and empower workers	Department of Labor	180 days	COMPLETE	Released resources for job seekers, workers, and tech vendors and creators on how AI use could violate employment discrimination laws	Equal Employment Opportunity Commission	(none)	COMPLETE
Announced the funding of new Regional Innovation Engines (NSF Engines), including with a focus on advancing AI	National Science Foundation	150 days	COMPLETE	Identified -- and shared with appropriate agencies -- best practices for federal law enforcement agencies to hire professionals with technical skills and train professionals in the responsible use of AI	Office of Personnel Management	180 days	COMPLETE	Released for comment a draft policy on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence	Office of Management and Budget	(none)	COMPLETE
Released an RFI on how federal agencies' privacy impact assessments may be more effective at mitigating privacy risks, including those that are further exacerbated by AI and other advances in technology and data capabilities	Office of Management and Budget	180 days	COMPLETE	Published a plan that addresses the use of AI and automated systems by states and localities in public benefits administration	Department of Health and Human Services	180 days	COMPLETE	Launched the Educational initiative, in order to prioritize AI-related workforce development	National Science Foundation	(none)	COMPLETE
Established an office to coordinate development of AI and other critical and emerging technologies across the agency	Department of Energy	180 days	COMPLETE	Issued guidance to state, local, territorial, and Tribal governments addressing the use of AI and automated systems in public benefits administration	Department of Agriculture	180 days	COMPLETE	Defined AI as a focus area for prize funds through the 2024 Growth Accelerator Fund Competition	Small Business Administration	(none)	COMPLETE
Published a final rule to strengthen the integrity of the H-1B program and enhance its use, including by experts in AI and related fields	Department of Homeland Security	180 days	COMPLETE	Published guidance on the application of nondiscrimination laws to advertisements of housing-related transactions on digital platforms, including through the use of algorithms	Department of Housing and Urban Development	180 days	COMPLETE	Confirmed the eligibility of AI-related expenditures for support via key programs that benefit small businesses	Small Business Administration	(none)	COMPLETE
Published new policy guidance for international students, clarifying and modernizing this pathway for experts in AI and other critical and emerging technologies	Department of Homeland Security	180 days	COMPLETE	Published guidance on the use of tenant screening systems -- including ones that use algorithms -- in ways that avoid unlawful	Department of Housing and Urban Development	180 days	COMPLETE	Published an RFI on AI's implications for global development	U.S. Agency for International Development & Department of State	(none)	COMPLETE
Incorporated NIST's AI Risk Management Framework, and other AI-related guidance, into security guidelines covering critical infrastructure	Department of Homeland Security	180 days	COMPLETE	Developed a strategy for ensuring the safety and effectiveness of AI deployed in the health care sector	Department of Health and Human Services	180 days	COMPLETE	Published an RFI to inform the development of the Global AI Research Agenda	U.S. Agency for International Development & Department of State	(none)	COMPLETE
Piloted new AI tools to identify and close vulnerabilities in critical government systems and software	Department of Defense & Department of Homeland Security	180 days	COMPLETE	Announced a new final rule and engaged with health care providers to affirm and promote understanding of federal nondiscrimination laws applicable to health care, including as related to AI	Department of Health and Human Services	180 days	COMPLETE	Published updated policy guidance regarding international student visas applicable to students in AI-related fields	Department of Homeland Security	(none)	COMPLETE
Evaluated -- and submitted a report to the President that discusses -- AI's potential to cause or exacerbate chemical, biological, radiological, and nuclear threats, as well as its ability to help counter such threats	Department of Homeland Security	180 days	COMPLETE	Directed further exploration -- including future public consultation -- of AI's challenges and opportunities related to transportation	Department of Transportation	180 days	COMPLETE	Proposed a new rule to provide for penalties and redress when AI is used to impersonate an individual for commercial purposes	Federal Trade Commission	(none)	COMPLETE
Developed a framework for nucleic acid synthesis screening to reduce the risk of misuse of synthetic biological products in research and development	Office of Science and Technology Policy	180 days	COMPLETE	Developed guidance on the use of generative AI by the federal workforce	Office of Personnel Management	180 days	COMPLETE	Proposed changes to a privacy rule that would further limit companies' ability to monetize children's data, including by limiting targeted advertising	Federal Trade Commission	(none)	COMPLETE
Launched an effort to engage the nucleic acid synthesis industry on necessary technical implementation details to facilitate adoption of the screening framework established per the Executive Order	Department of Commerce	180 days	COMPLETE	Created a resource guide for federal AI acquisition	General Services Administration	180 days	COMPLETE	Issued an advisory opinion to highlight that false, incomplete, and old information must not appear in background check reports, including for tenant screening	Consumer Financial Protection Bureau	(none)	COMPLETE
Established a training program to help industry and domestic law enforcement better understand and respond to AI-related IP theft	Department of Homeland Security	180 days	COMPLETE	Submitted a report to the President on progress made -- and recommendations for -- increasing AI capacity	AI and Tech Talent Task Force	180 days	COMPLETE				
Increased information sharing related to AI technology theft, AI-enabled IP theft, and AI-enabled digital piracy with state, local, and international law enforcement, including the European Union Intellectual Property Office, Interpol, and Europol	Department of Homeland Security	180 days	COMPLETE	Established guidance for skills-based AI-related hiring	Office of Personnel Management	180 days	COMPLETE				
				Established an interagency working group to facilitate federal AI-related hiring	Office of Personnel Management	180 days	COMPLETE				

\*Actions added to the summary table since its publication on March 28 are **bolded**.



# What next?

BY [MATT O'BRIEN](#) AND [BARBARA ORTUTAY](#)

Updated 4:39 PM PST, November 20, 2024



SAN FRANCISCO (AP) — President-elect Donald Trump [has vowed to repeal](#) President Joe Biden's signature artificial intelligence policy when he returns to the White House for a second term.

What that actually means for the future of AI technology remains to be seen. Among those who could use some clarity are the government scientists and AI experts from multiple countries gathering in San Francisco this week to deliberate on AI safety measures.

Trump promised in his presidential campaign platform to “repeal Joe Biden’s dangerous Executive Order that hinders AI Innovation, and imposes Radical Leftwing ideas on the development of this technology.”

But he hasn’t made clear what about the order he dislikes or what he’d do about the AI Safety Institute. Trump’s transition team didn’t respond to emails this week seeking comment.

Would these guidelines change under the Trump administration or with Elon Musk? xAI's Grok has been noted to generate harmful content more easily than models from other companies. One of my friends in xAI mentioned that xAI prioritizes catching up with OpenAI over current safety concerns and Elon does not seem to put emphasis on safety so much. Furthermore, Elon has been critical of models tuned so that the models hold liberal people's opinions. Could the upcoming shift in leadership could potentially lead to a reevaluation of priorities?  
— Kazusato

# Conclusion/Takeaways

- This executive order set a framework for safe, secure, and trustworthy development and use of AI
- Collaboration, innovation, and safeguards must work in tandem
- Role of government, private sector, academia is crucial



# Concluding Discussion Questions

**What sections of the Executive Order do you think are effective/promising? Are there any sections you find lacking or areas where it could be improved? Is anything missing?**

1. Given the Executive Order's emphasis on safeguarding privacy and addressing AI-related risks, what role should international collaboration play in establishing standardized guidelines for AI governance, and how might differing global privacy laws impact this effort? – **Baifeng**
2. While this executive order has not mentioned anything about open models, I wonder whether open models would help achieve the standards proposed, such as privacy and safety. – **Brandon**
3. There seems to be an interesting focus on "biological sequence data", even though there are many other types of training data that could lead to harmful AI systems (e.g trained on radioactive materials databases, etc.). I wonder why this focus/wording was chosen that way. – **Sanjeev**
4. How might the Federal Government address potential conflicts of interest or "revolving door" dynamics between policymakers, regulators, and private AI companies, ensuring that regulations are both robust and free from undue influence by industry stakeholders? – **Jerome**