Building a better working world

Biden administration news alert

Executive Order: Safe, Secure, and Trustworthy Artificial Intelligence

31 October 2023

On 30 October, President Biden issued a sweeping executive order ("Executive Order" or EO) on artificial intelligence (AI) with the goal of promoting the "safe, secure, and trustworthy development and use of artificial intelligence." A White House fact sheet on the order can be found here.

This Executive Order represents a significant contribution to the subject of accountability in how AI is developed and deployed across organizations. Given the breadth of recommendations and actions provided, it is likely to have an effect on organizations across all sectors of the economy, from the most mature AI implementers to first-time adopters. The Executive Order's definition of AI systems is also broad; it is not limited to generative AI or systems leveraging neural networks but is inclusive of systems which have been built over the last several years.

Determining the extent to which the EO affects an organization will involve careful assessment of not only an entity's own use of AI, but also the extent to which its products and services incorporate or are reliant on third-party vendors' AI-enabled capabilities.

Importantly, the National Institute of Standards and Technology (NIST) will be foundational in the development of guidelines and best practices for "developing and deploying safe, secure and trustworthy AI systems," and companies may consider evaluating their existing AI risk management frameworks against the NIST AI Risk Management Framework to develop a baseline and prepare for additional guidance to be released from relevant agencies and regulatory bodies.

The Executive Order is guided by eight principles and priorities:

1. AI must be **safe and secure** by requiring robust, reliable, repeatable and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, mechanisms to test, understand, and mitigate risks from these systems before they are put to use.
2. The US should promote **responsible innovation, competition and collaboration** via investments in education, training, R&D and capacity while addressing intellectual property rights questions and stopping unlawful collusion and monopoly over key assets and technologies.
3. The responsible development and use of AI require a **commitment to supporting American workers** though education and job training and understanding the impact of AI on the labor force and workers' rights.
4. AI policies must be consistent with the advancement of **equity and civil rights**.

5. The **interests of Americans who increasingly use, interact with, or purchase** AI and AI-enabled products in their daily lives must be protected.
6. **Americans' privacy and civil liberties must be protected** by ensuring that the collection, use and retention of data is lawful, secure and promotes privacy.
7. It is important to manage the risks from the federal government's own use of AI and **increase its internal capacity to regulate, govern and support responsible use of AI** to deliver better results for Americans.
8. The federal government should lead the way to global societal, economic and technological progress including by **engaging with international partners** to develop a framework to manage AI risks, unlock AI's potential for good and promote a common approach to shared challenges.

Notably, the EO uses the definition of "artificial intelligence," or "AI," found at 15 U.S.C. 9401(3):

> *"a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."*

Therefore, the scope of the EO is not limited to generative AI; any machine-based system that makes predictions, recommendations or decisions is impacted by the EO.

As expected, the **NIST** is tasked with a leading role in implementing many of the directives of the EO. The NIST is called upon to lead the development of key AI guidelines, and the NIST AI Risk Management Framework is repeatedly referenced in the Executive Order. However, the EO adopts the "all-of-government approach" that has become a trademark of the Biden administration, tapping agencies and offices across the entire administration to tackle the use of AI technologies in their areas of expertise with numerous actions specified in the near and medium term.

With Congress continuing to study the policy implications raised by AI technologies, this Executive Order and the actions that follow will be the cornerstone of the federal regulatory approach in the space for now. Of course, these actions are limited to the authorities of the executive branch, so this EO concentrates its mandates on programs administered by federal agencies, requirements for AI systems procured by the federal government, mandates related to national security and critical infrastructure, and launching potential rulemakings that govern regulated entities. This EO, like all executive orders, cannot create new laws or regulations on its own, but can trigger the beginning of such processes.

Key provisions of the EO are summarized below.

Key highlights

Safety and security

- The EO directs the NIST, working with the Department of Commerce, to develop two sets of guidelines within 270 days:
  - First, the NIST is directed to establish guidelines and **best practices for "developing and deploying safe, secure, and trustworthy AI systems**."
  - Additionally, the NIST is called upon to develop standards and procedures for developers of AI (outside of national security applications) to conduct **AI red-teaming tests** (structured testing to identify potential flaws and vulnerabilities).

- The Department of Energy (DoE), also within 270 days, is directed to develop and implement "a plan for developing the Department of Energy's AI model evaluation tools and AI testbeds" including evaluating AI tools where outputs "may represent nuclear, nonproliferation, biological, chemical, critical-infrastructure, and energy-security threats or hazards."

- Specifically with regard to the deployment of **dual-use foundation models** (AI models trained on broad data and applicable in a wide range of contexts), the EO **invokes the Defense Production Act** to impose mandates:
    - The Commerce Department will establish requirements (within 90 days) for "companies developing or demonstrating an intent to develop potential dual-use foundation models" to report certain information and activities to the federal government.
    - Entities will also be required to provide the federal government with specific information about any **large-scale computing cluster**.

- Specifically with regard to dual-use foundation models with widely available model weights (e.g., **Open Source Large Language Models**):
    - The secretary of Commerce shall (within 270 days), solicit input from the private sector, academia, civic society, and other stakeholders through a public consultation process on potential risks, benefits and other implications.
    - Based on consultations, the secretary of Commerce shall submit a report to the president on the potential benefits, risks and implications as well as policy and regulatory recommendations pertaining to these models.

- Following up on previous cybersecurity efforts, the EO directs the secretary of Commerce (within 90 days) to propose regulations requiring **Infrastructure as a Service** (IaaS) providers to notify the Department "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."
    - US IaaS providers will be further prohibited from permitting foreign companies to resell their services or open accounts for foreign persons unless they agree to make similar disclosures in the future.

- With respect to **critical infrastructure**, the heads of federal agencies that supervise critical infrastructure must make an assessment and report to the secretary of Homeland Security the "potential risks related to the use of AI in critical-infrastructure sectors involved, including ways in which deploying AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyber-attacks, and shall consider ways to mitigate these vulnerabilities."
    - The Treasury Department is required to issue a report within 150 days on best practices for financial institutions to manage AI-specific cybersecurity risks for **financial institutions**.
    - The EO also outlines a process to mandate the adoption by critical infrastructure owners and operations of the NIST AI Risk Management Framework via "appropriate regulatory action."

- The EO also recognizes the potential for AI technologies to promote cybersecurity defenses, calling on the Departments of Homeland Security and Defense to conduct studies and issue reports on how AI can be used to aid in cyber defense.

- With respect to **Chemical, Biological, Radiological, and Nuclear (CBRN) threats**, the Department of Homeland Security (DHS), along with the Office of Science and Technology Policy (OSTP) and DoE, is directed to conduct a 180-day evaluation of the potential for AI to be used in making CBRN threats – while also studying how the technology could be deployed to defend against such threats.
    - Likewise, the Department of Defense (DoD) – working with the administration, OSTP and the National Academies of Sciences, Engineering and Medicine – will conduct a 120-day study on the ways AI can both increase and counter biosecurity risks.
    - Additional mandates are set forth regarding the risk of misuse of synthetic nucleic acids and to "improve biosecurity measures for the nucleic acid synthesis industry."

- Finally, the EO calls for the drafting of an interagency National Security Memorandum on AI to "address the governance of AI used as a component of a national security system or for military and intelligence purposes" through a coordinated executive branch effort.

Federal procurement of AI systems

As the largest customer in the US economy, the federal government's own purchasing requirements often become industry standard – making procurement policy a very strong tool for promoting policy goals.

- The Office of Management and Budget (OMB) is required by the EO to set up **an interagency council on the use of AI in federal government operations** (outside of national security systems). OMB's director must issue, within 150 days, "guidance to agencies to strengthen the effective and appropriate use of AI, advance AI innovation, and manage risks from AI in the Federal Government." In addition to other provisions that guidance must include (in part):
    - Requiring the designation of a Chief Artificial Intelligence Officer at each agency
    - At some agencies, the creation of an internal Artificial Intelligence Governance Board
    - Risk management practices for government use of AI that impacts "people's rights or safety" (utilizing, as appropriate, the NIST AI Risk Management Framework)
    - Recommendations regarding AI testing, labeling AI output, and the "independent evaluation of vendors' claims concerning both the effectiveness and risk mitigation of their AI offerings."

- OMB is further tasked with establishing systems to ensure agency compliance with guidance on AI technologies, including ensuring that agency contracts for the purchase of AI systems align with all requirements and a yearly cataloging of agency AI use cases.

- Specifically with regard to the use of generative AI systems by the federal government, "agencies are discouraged from imposing broad general bans or blocks on agency use of generative AI" but instead are urged to put appropriate safeguards in place to utilize generative AI "at least for the purposes of experimentation and routine tasks that carry a low risk of impacting Americans' rights."
    - The administrator of General Services, along with OMB, is tasked with developing a framework for the use of generative AI by the federal workforce.

- The Executive Order tasks OMB and OSTP with determining "priority mission areas for increased Government AI talent" as well as the convening of a Technology Talent Task Force to accelerate the hiring of AI talent across the federal government. The Task Force will identify and circulate "best practices for agencies to

attract, hire, retain, train, and empower AI talent, including diversity, inclusion, and accessibility best practices, as well as to plan and budget adequately for AI workforce needs."

- The Office of Personnel Management (OPM) is authorized to consider hiring tools for these AI professionals, including direct hire authority for AI roles, pay flexibilities, personnel vetting requirements, pooled hiring and incentive pay programs.
- Agencies are also required to implement (or increase) training programs to educate the current federal workforce on AI issues.
- A separate study of the AI personnel needs of the DoD is required within 180 days, with DoD and the DHS encouraged to "work together to enhance the use of appropriate authorities for the retention of certain noncitizens of vital importance to national security."

AI-generated content

- The EO seeks to advance technology to identify, authenticate and trace content produced by AI systems.
  - The Department of Commerce is directed to complete a 240-day study of the existing tools and methods to detect AI-generated content, track its provenance and prevent AI technology from producing Child Sexual Abuse Material.
  - Using that information, the Department will have 180 days to develop guidance on "**digital content authentication and synthetic content detection measures.**"
  - Finally, following up on that guidance, the OMB is required to issue guidance to federal agencies for labeling and authenticating official US government content.

- The **US Patent and Trademark Office** (PTO) is required by the EO to provide guidance to patent examiners on issues of "inventorship and the use of AI" and, potentially, issues of patent eligibility.

- Similarly, the EO directs the **US Copyright Office** to perform a 270-day study of the copyright issues raised by AI technology, "including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training."
  - To combat intellectual property crimes through AI technologies, DHS is directed to develop a training, analysis, and evaluation program" and share information with the Federal Bureau of Investigation, Customs and Border Protection and other agencies.

Promoting innovation

- To ensure that the US has the available talent needed to lead in the development of AI technology, the EO calls for the **streamlining of processes** for noncitizens to "work on, study, or conduct research in AI or other critical and emerging technologies."
  - The secretaries of State and Homeland Security are further directed to consider rulemakings and efforts to expand existing programs for highly skilled foreign talent.
  - The Department of Labor is tasked with identifying AI and other STEM-related occupations for which there are insufficient US workers.

- The EO calls for the National Science Foundation (NSF) to establish a **National AI Research Resource** (NAIRR) to facilitate collaboration between the government and private sector. In line with the recommendations of the NAIRR Task Force, the program will "pilot an initial integration of

distributed computational, data, model, and training resources to be made available to the research community in support of AI-related research and development."

- The NSF is also called on to establish, within 150 days, at least one NSF Regional Innovation Engine that prioritizes work on AI technology, as well as four new National AI Research Institutes (within 540 days).
- Additional government investments in promoting AI innovation are mandated at:
  - DoE (to enhance existing training programs for AI scientists; utilize AI to combat climate change; report on the potential for AI to improve the electric grid infrastructure)
  - Department of Health and Human Services (to prioritize programs to support responsible AI development and use in programs that improve "clinical care, real-world-evidence programs, population health, public health, and related research," including in underserved communities)
  - Department of Veterans Affairs (to use AI to improve veterans' health care and promote small business innovation)
  - President's Council of Advisors on Science and Technology (to study the potential for AI to tackle "major societal and global challenges")

Competition

- Continuing the administration's focus on competition issues, the EO directs all federal agencies to use their authorities to **promote competition in AI** and related technologies.
  - Included in the mandate are actions such as "addressing risks arising from concentrated control of key inputs, taking steps to stop unlawful collusion and prevent dominant firms from disadvantaging competitors, and working to provide new opportunities for small businesses and entrepreneurs."

- Some agencies are tasked with specific directives promoting competition:
  - The Federal Trade Commission (FTC) is required to consider using its rulemaking authority over the marketplace to "ensure that consumers and workers are protected from harms that may be enabled by the use of AI."
  - The Department of Commerce is directed to take measures that **promote competition in the semiconductor sector**, which is crucial to powering AI technologies.
  - The EO requires the Small Business Administration (SBA) to allocate funding for AI initiatives and ensure that grant programs are eligible for AI-related small businesses.

Worker protections

- The potential for AI-fueled technologies to displace workers has been a key concern of policymakers, and several related reports are mandated by the EO, including:
  - A study by the Council of Economic Advisors on the "labor-market effects of AI"
  - An evaluation by the secretary of Labor on the potential for AI-related displacements in the federal workforce
  - The development of employer principles and best practices by the Department of Labor on militating the potential harm/maximizing the benefits of AI technologies for workers

- Additionally, NSF is required to prioritize AI-related workforce development through its existing programs.

Civil rights and equity

- The Executive Order calls on federal agencies to ensure that AI technologies do not promote bias and discrimination in a wide array of areas. Coordinated by the Assistant Attorney General for the Civil Rights Division of the Department of Justice, the EO:
  - Requires a study of the use of AI in the **criminal justice system** (sentencing, parole, bail, prison management, etc.) from the Attorney General within one year
  - Recognizes the potential for AI to "enhance law enforcement efficiency and accuracy, consistent with protections for privacy, civil rights, and civil liberties"
  - Calls on an interagency working group to promote the hiring and training of law enforcement AI professionals

- With respect to government programs, agencies are required to ensure that AI technology does not result in **discrimination in the administration of benefit programs**.
  - The Department of Health and Human Services (HHS) is required to publish a plan on the use of AI systems by states and localities administering federal government programs to ensure the "access to benefits by qualified recipients; notice to recipients about the presence of such systems; regular evaluation to detect unjust denials; processes to retain appropriate levels of discretion of expert agency staff; processes to appeal denials to human reviewers; and analysis of whether algorithmic systems in use by benefit programs achieve equitable and just outcomes."
  - Similarly, the Department of Agriculture is directed to publish guidance for public benefits administrators who use AI systems in the implementation of their programs.

- Other federal agencies are directed to take action to prevent discrimination and bias from the use of AI systems as well:
  - The Department of Labor (DoL) has a mandate to publish guidance for federal contractors regarding nondiscrimination in **hiring** involving AI and other technology-based systems.
  - The Federal Housing Authority and Consumer Financial Protection Bureau (CFPB) are directed to use their authorities to prevent bias in the **housing and consumer financial markets**, including in the areas of underwriting and appraisals.
  - The Department of Housing and Urban Development (HUD) and the CFPB are also tasked with examining the use of AI in the **property rental market**, including AI systems for tenant screening and the advertising of housing and credit.
  - The Architectural and Transportation Barriers Compliance Board is directed to ensure that **people with disabilities** are not subject to unequal treatment by AI systems that use biometric data.

Consumer protection, privacy and health care

- Protecting American consumers from fraud is a mandate of the EO, which directs agencies to consider "clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and requirements and expectations related to the **transparency of AI models and regulated entities' ability to explain their use of AI models**."

- In the **health care** sector, HHS is directed to work with other agencies in establishing an HHS Task Force to develop a strategic plan on the use of AI in areas including research and discovery, drug and device safety, health care delivery and public health.
    - After a detailed 180-day study mandated by the EO, HHS is required to:
        - Issue a strategy on whether AI technologies in the health and human services sector "maintain appropriate levels of quality."
        - Take appropriate actions to ensure that health care providers who receive federal funding comply with nondiscrimination requirements when utilizing AI technology.
    - In the future, HHS policies are required to be issued regarding the occurrence of clinical errors when utilizing AI technology and the use of AI in the drug development process.

- While the US has yet to enact national consumer data protection legislation, the EO takes steps to protect commercially available information (CAI) held by federal agencies. Additionally, the EO directs the **Department of Justice** (DoJ) to launch a regulatory proceeding to gather feedback on "how privacy impact assessments may be more effective at mitigating privacy harms, including those that are further exacerbated by AI."
    - The Department of Commerce and NIST are required to issue guidelines for agencies, within a year, to promote the use of privacy-enhancing technologies (PETs).
    - DoE and the NSF are directed to create a Research Coordination Network dedicated to PET research and encourage the incorporation of privacy-enhancing technologies.

Global leadership

- In its closing pages, the EO seeks to "strengthen United States leadership of global efforts to unlock AI's potential and meet its challenges" by requiring government leaders to engage internationally and participate in multi-stakeholder, collaborative efforts.
    - The administration emphasizes the values of the voluntary commitments made by US technology companies, saying that the US should seek to "establish a strong international framework for managing the risks and harnessing the benefits of AI, including expanding and internationalizing voluntary actions made by United States companies."
    - The EO also requires the Secretaries of Commerce and State to work with key international partners on global technical standards, mandating a report within 270 days on a plan for global engagement.

Additional

The EO addresses a number of additional issues not summarized above, but which will be critically important to some developers and deployers of AI technology. Other topics covered by the EO include:

- Dual-use foundation models with widely available model weights (Section 4.6)
- Protections surrounding the use of federal data sets to train AI systems (Section 4.7)
- The creation of an Artificial Intelligence Safety and Security Advisory Board at the DHS to provide "advice, information, or recommendations for improving security, resilience, and incident response related to AI usage in critical infrastructure." (Section 4.3(a)(v))
- The creation of an interagency White House AI Council tasked with coordinating the activities across the federal government related to the implementation of this Executive Order.

- The use of AI in the transportation sector, including AI enhancements to autonomous vehicle systems. (Section 8(c))
- Education and AI, including the development of an AI Toolkit for education leaders (Section 8(d))
- The potential for AI to impact communications networks, improve spectrum management, network security, and interoperability. The EO singles out "efforts to combat unwanted robocalls and robotexts that are facilitated or exacerbated by AI" as an area for potential rulemaking. (Section 8(e))
- Priority use of the federal government's Technology Modernization Fund for AI projects (Section 10.1(g))

For information on the US public policy debate surrounding AI, please see our EY publication *US public policy spotlight: artificial intelligence*. For a discussion of global AI policy trends, please see *How to navigate global trends in Artificial Intelligence regulation*.

For questions about public policy:

Contacts:
Bridget Neill
EY Americas Vice Chair, Public Policy
bridget.neill@ey.com

John Hallmark
Principal, EY US Political and
Legislative Leader, Ernst & Young LLP
john.hallmark@ey.com

For questions about AI:

Contacts:
Richard Jackson
EY Global AI Assurance Leader
Ernst & Young LLP
richard.jackson@ey.com

Dan Diasio
EY Global AI Consulting Leader
dan.diasio@ey.com

Rani Bhuva
Partner, EY Americas Business Consulting, Ernst & Young LLP
rani.bhuva@ey.com

Ryan Doherty
Partner, EY Americas Technology Consulting, Ernst & Young LLP
ryan.doherty@ey.com

Khalid Khan
Partner, EY-Parthenon, Ernst & Young LLP
khalid.khan1@parthenon.ey.com