ALERT

President Biden Issues Long-Awaited Executive Order on Safe, Secure and Trustworthy Artificial Intelligence

By The Honorable Jerry McNerney, Elizabeth Vella Moeller, Aaron M. Oser, Brian E. Finch, Brooke L. Daniels, Tony Phillips, Benjamin J. Cote, Lee G. Petro, Samantha Franks, Amaris Trozzo

TAKEAWAYS

- The Executive Order creates new guidelines directed toward AI safety and security, privacy protections, equity and civil rights, consumers' and workers' rights, and innovation and competition.
- Provisions of the Order leverage the power of the Defense Production Act to require certain companies developing AI products that could impact national security, economic security or public health and safety, to regularly report to the government about training their models and security measures, as well as to share the results of all red-team safety tests.
- Congress also recently introduced the Artificial Intelligence Advancement Act of 2023, which would establish artificial intelligence bug bounty programs and require reports and analyses on a variety of AI-use cases.

11.01.23

On October 30, President Biden issued the long-awaited Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (AI), the first order to navigate AI's impact across sectors and to help agencies and consumers harness the benefits of AI while mitigating risks.

Executive Action on AI

President Biden first addressed AI in the Blueprint for an AI Bill of Rights in October 2022. Since then, executive agencies have worked to incorporate the AI Bill of Rights principles into their enforcement activity,

prioritizing protecting consumers from potential AI harms that fall within their agency's jurisdictions. The Administration also secured voluntary agreements from several leading generative AI companies in August to promote safety, security and public trust in generative AI.

The Federal Communications Commission (FCC) has demonstrated the Executive Order's interest in AI, having recently held a hearing with the National Science Foundation on July 13, 2023, to discuss many cross-cutting AI issues. The FCC is also considering the adoption of a Notice of Inquiry at its November 2023 meeting to study whether it should adopt rules to protect consumers from unwanted and illegal telephone calls and text messages generated through the use of AI technologies.

These actions have built up to the much-anticipated Executive Order. In addition, Vice President Harris and Secretary of Commerce Raimondo are traveling to the AI Safety Summit 2023 at Bletchley Park, UK, where the Vice President will give a speech outlining the administration's Executive Order and vision for the future of AI.

The Executive Order on Artificial Intelligence

Overview of the Order

The Executive Order will leverage the regulatory powers of multiple federal agencies to (a) monitor risks stemming from AI use and programs, (b) develop new and innovative uses for the technology, and (c) implement these new technologies safely. The Order sets out to promote the safe, responsible, and ethical use of AI by federal agencies and to protect consumers through existing regulatory authorities.

Companies using or developing AI who contract with the federal government or are regulated will want to monitor the variety of standards created under the Executive Order. For example, the Department of Commerce is tasked with creating watermarking standards that may be further incorporated into the Federal Acquisition Regulation for government procurements. Companies may also want to be mindful of the Department of Energy's efforts to test and address chemical, biological, nuclear and other potential AI risks. In addition, the National Institute of Standards and Technology (NIST) will develop two sets of guidelines. The first, to support the goal of promoting industry standards, will include a companion resource to the AI Risk Management Framework, a companion resource to the Secure Software Development Framework and benchmarks for auditing AI capabilities. The second set of guidance will outline the processes and procedures for red-team testing AI systems.

The Executive Order also addresses Congress, asking them to develop and pass data privacy legislation. While not introduced yet this year, the American Data Privacy and Protection Act (ADPPA) garnered attention as a promising vehicle for a federal framework in 2022. Introduced originally by Rep. Pallone (D-NJ-6) and Rep. McMorris Rodgers (R-WA-5), the ADPPA would establish a national framework to protect

consumer data privacy and security and bolster the privacy rights of individual rights. As Chair of the Energy and Commerce Committee, Congresswoman Rodgers will serve an important role in developing privacy regulation moving forward.

The Defense Production Act

Importantly, the Executive Order also leverages the Defense Production Act (DPA) to require companies developing or intending to develop "dual-use foundation models" to report the results of any red-team safety tests to the government, as well as to notify the government when they are training their models. These companies are compelled to report to the Department of Commerce their physical and cybersecurity plans to protect the integrity of the training process and model weights from outside threats.

A dual-use foundation model is defined in the Executive Order as a 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…"

The Order also also exercises authority pursuant to the International Emergency Economic Powers Act to require Infrastructure as a Service (IaaS) products, or cloud services, to report to the Secretary of Commerce when a foreign person rents server space to train large AI models. Under this provision, U.S. IaaS providers must prohibit their foreign resellers from providing the U.S. IaaS product unless the foreign reseller reports each instance in which a foreign person transacts for the U.S. IaaS product. The Secretary of Commerce has 90 days to propose regulations on the reporting requirements. Within 180 days, Commerce will propose regulations for U.S. IaaS providers to ensure that the foreign resellers verify the identity of any foreign person that obtains an IaaS account.

Executive Order Details

The Executive Order establishes a White House Artificial Intelligence Council to coordinate all executive branch activities on AI. The deputy chief of staff for policy will chair the council and direct the efforts of the agencies to carry out the mission of the Executive Order, which are detailed below.

- **Safety**

  The Executive Order mandates the development of guidelines, standards and best practices to promote AI safety and security.

  - Providers of dual-use foundational models will be required to notify the government when they are training their AI models and report their safety testing results under the Defense Production Act.
  - The National Institute of Standards and Technology is directed to develop standards, tools and tests to ensure that AI systems are safe, secure and trustworthy before being deployed.
  - The National Institute of Standards and Technology is directed to develop standards, tools and tests to ensure that AI systems are safe, secure and trustworthy before being deployed.

- The Department of Homeland Security will establish an AI Safety and Security Board. This Board will be comprise experts from the private sector, academia and government and will provide advice and recommendations to improve safety, resilience and incident response plans for the use of AI in critical infrastructure.
- The National Security Council is directed to create a National Security Memorandum that ensures the military and the intelligence community use AI safely, ethically and effectively.
- The Department of Energy will establish AI testbeds to assess near-term extrapolation of AI system capabilities and identify nuclear, nonproliferation, biological, chemical, critical infrastructure and energy-security threats and hazard and prepare guardrails that protect against these risks.

- **Cybersecurity**

  The Executive Order promotes the use of AI technologies to protect against cyber threats.

  - The Executive Order will capitalize on the AI Cyber Challenge to develop tools that leverage AI to find and fix vulnerabilities.
  - The Department of Treasury is required to submit a public report outlining best practices for the financial sector to manage cybersecurity risks.
  - The Department of Homeland Security and the Department of Defense are directed to each launch a pilot program testing the capabilities of AI technologies to discover and remediate vulnerabilities in government networks.
  - Companies developing dual-use foundation models will be required, under the Defense Production Act, to submit reports to the Secretary of Commerce outlining how they secure the integrity of their training processes and model weights from potential cyber threats.

- **Transparency**

  The Executive Order aims to understand the risks posed by synthetic content and reduce risks by fostering capabilities to identify synthetic content.

  - The Department of Commerce will establish guidance for content authentication and watermarking to distinguish AI-generated content. Federal agencies are directed to use watermarking tools as well.
    - The Federal Acquisition Regulatory Council is encouraged to incorporate the guidance created by the Department of Commerce on how to distinguish synthetic content into procurement requirements, which may eventually require companies using generative AI contracting with the government to employ watermarking or other labeling mechanics themselves.
  - Under the Department of Commerce, the National Telecommunications and Information Administration is directed to report on the risks and benefits for model weights—the parameters adjusted during training of models and the mechanism by which models learn from a training set—that are open-source or published online.

- **Privacy**

  The Executive Order directs activity that will protect Americans' privacy and civil liberties as AI continues to advance.

  - The EO calls on Congress to pass bipartisan data privacy protection legislation.
  - The Order directs federal agencies to prioritize supporting projects that develop or accelerate the use of privacy-preserving techniques, including tools that use cutting edge AI technologies.
  - The Director of the Office of Management and Budget (OMB) will conduct a survey of the personally identifiable information (PII) procured by agencies, including information procured or processed indirectly through vendors. The results of this survey will inform future strategies to mitigate privacy risks. The Order directs the OMB to issue a Request for Information (RFI) within 180 days of the Order to solicit feedback on how privacy impact assessments can be more effective and directs the agencies to take the necessary steps to carry out the strategy identified through the RFI process.
  - The Order will create a Research Coordinating Network to advance rapid breakthroughs and developments on privacy technologies, which will coordinate with the National Science Foundation to leverage privacy-preserving technologies for federal use.
  - The Order will establish guidelines for federal agencies to evaluate the effectiveness of privacy-preserving techniques.

- **Immigration**

  The Executive Order seeks to attract foreign AI talent and lower barriers to entry.

  - The State Department and Department of Homeland Security are directed to streamline Visa applications for immigrants with AI expertise. The State Department will also create rules to allow foreign nationals in the U.S. to work on AI and emerging tech without "unnecessary interruption."
  - The State Department, Department of Commerce and the White House Office of Science and Technology Policy will work together to attract and retain AI experts and promote science and technology work by developing new resources and reports advertising U.S. capabilities.

- **Competition**

  One objective of the Executive Order is to create an open and competitive AI market that prioritizes U.S. innovation and supports small companies coming to market.

  - In order to support a fair, open, and competitive AI system, the Order directs agencies to provide technical assistance to small developers and entrepreneurs to help with commercial breakthroughs.
    - The Department of Commerce is also directed to retain a "flexible membership structure" for smaller semiconductor companies to participate in the National Semiconductor Technology Center.
    - The Department of Commerce is directed to create mentorship programs to increase interest in the semiconductor industry.

- The Order authorizes a pilot program implementing the National AI Research Resource (NAIRR) and expands grants for AI research into health care and climate change. NAIRR was established under the National AI Initiative Act of 2020, which directed the National Science Foundation and the Office of Science and Technology Policy to create a task force to discover the feasibility of a national research resource that would expand access to critical data for those engaged in AI development. The NAIRR Task Force produced a final report to Congress, but NAIRR has not yet received federal funding.
- The Federal Trade Commission is directed to counter anti-competitive behavior in the AI industry as well as address consumer harm.
- Companies developing dual-use foundational models will be required to regularly report their technology protection plans to the Department of Commerce. These plans may include details about how the owner mitigates risks, such as espionage, that could impact U.S. competitiveness.
- Addressing the concern of foreign adversaries accessing U.S. AI technologies, the Order also directs cloud services to notify the government when server space is rented by foreign persons or entities to train large AI models.

- **Copyright**

  The Executive Order addresses novel intellectual property questions and actions to protect investors and creators.

  - The Patent and Trademark Office will provide guidance for patent examiners and applicants on how to address AI in applications. The Office will have 120 days to provide guidance on the use of AI in the inventive process and how inventorship issues can be analyzed in various scenarios. The Office will then have a subsequent 150 days to address other issues at the intersection of AI and IP, for example patent eligibility.
  - The Office will recommend actions the Executive can take to protect works generated or created by AI as well as the works used to train AI models.

- **Labor**

  The Executive Order cites a commitment to supporting American workers in the AI transition.

  - The Council of Economic Advisors will draft a report within 180 days documenting the effects of AI on the labor market.
  - The Department of Labor is tasked with drafting and publishing a report for the President identifying opportunities for the federal government to support workers facing labor disputes and bolster worker protections.
  - The Secretary of Labor will develop principles and best practices for employers to mitigate potential harms to their employees, including by addressing job-displacement risks, labor standards and job quality (including issues related to equity), and confirming the rights of employees regarding the information collected on them or used by their employers. The Secretary is also directed to issue guidance confirming that employers who deploy AI to monitor or augment an employee's work must comply with protections under the Fair Labor Standards Act.

- The Office of Personnel Management is tasked with developing a government policy or guardrails for the use of generative AI in the federal workplace. The Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget, in consultation with others, will develop plans to increase AI talent in the government and advance the capacity of the federal AI workforce, using existing talent programs where possible.

- **Equity and Civil Rights**

  The Executive Order works to protect and prioritize equity throughout all government initiatives

  - The Order requires agencies to provide clear guidance to landlords, federal benefit programs and federal contractors on how to prevent AI algorithms from engaging in discrimination.
  - The Department of Justice and federal civil rights offices will develop best practices for investigating and prosecuting AI civil rights violations. This will also involve additional training and technical assistance between the offices.
  - The Attorney General will create a report identifying how AI can be used fairly and safely in sentencing, parole and probation, pretrial release and detention, risk assessments, surveillance, crime forecasting and predictive policing, and forensic analysis. The report will also recommend best practices for law enforcement agencies to address concerns about AI's effect on equity and civil rights when deployed in these decisions.

- **Housing**

  The Executive Order endeavors to combat unlawful discrimination in decisions about access to housing and other real-estate transactions.

  - The Consumer Financial Protection Bureau (CFPB) may issue, and the Department of Housing and Urban Development (HUD) will issue, guidance on how the Fair Credit Reporting Act and the Equal Credit Opportunity Act apply to AI discrimination in advertising for housing or credit services. The guidance provided will also address tenant screening systems and how the use of certain data by AI systems can lead to discriminatory outcomes.

- **Health**

  The Executive Order promotes the responsible deployment of AI that accounts for the wellbeing of citizens and potential beneficial uses of AI in the health care sector.

  - The Department of Health and Human Services (HHS) will create an AI Safety Program to receive reports of unsafe health care practices involving AI and will develop a strategy to regulate the use of AI or AI-enabled tools in the health care sector.
  - The Department must establish an HHS AI Task Force that will publish, a year after its creation, a strategic plan on the responsible deployment of AI and AI-enabled technologies for the health sector.
  - The HHS will identify and prioritize grant opportunities for AI health technologies, including through the 2024 Leading Edge Acceleration Project, to explore ways to improve health care data.

- **Transportation**

  The Executive Order supports the safe integration of AI into the transportation sector.

  - The Department of Transportation will support pilot transport-related applications of AI and review the efficacy of these pilot programs to develop further recommendations or other regulatory actions for addressing AI integration.
  - The Department of Transportation will direct Advanced Research Project Agency-Infrastructure (ARPA-I) to explore and prioritize funding opportunities for AI transportation projects.

- **Education**

  The Order requires the Department of Education to address the safe, responsible and nondiscriminatory uses of AI in education through appropriate documents and resources.

  - The Department of Education will create an AI Toolkit to assist in implementing the recommendations made by the Department in the AI and the Future of Teaching and Learning report.

- **Telecommunications**

  The Federal Communications Commission is encouraged under the Order to consider how AI will affect communication networks and consumers.

  - The FCC may review how AI can improve network resiliency and spectrum efficiency as well as address unwanted robocalls. These measures could in turn influence the rollout of 5G and 6G technologies.

- **International Collaboration**

  The Executive Order promotes strategies to strengthen American leadership abroad.

  - The Department of State and the Department of Commerce are directed to establish a robust international framework, coined the Global AI Research Agenda, to harness AI benefits while managing AI risks.
  - The federal government will work with international partners and standards organizations to develop and implement AI standards, including multilateral agreements on security guidelines for critical infrastructure.

Ongoing Congressional Activity

The Executive is not alone in addressing AI, as members of Congress in both the House and Senate have turned their attention to AI legislation. While the Executive Order is limited to existing spending amounts and authorities, Congress can pass legislation to create new authorities and appropriate additional funding that can affect AI development. Members of both the House and Senate have been active in introducing legislation and holding hearings to lay the groundwork for AI legislation.

Notably, Senate Majority Leader Schumer (D-NY) announced his SAFE Innovation Framework in June and at the accompanying AI Forums, a series of meetings with senators and experts from industry and academia designed to educate the senators on the contours of AI technology. The first AI Forum was attended by 60 senators and hosted prominent AI company leaders. The second AI forum on Tuesday, October 24, focused

on AI innovation, which featured venture capitalists and company leaders working on next-generation AI systems as well as civil society groups. The next forum will be held on Wednesday, November 1, to focus on AI and the workforce.

Critical to AI legislation in the Senate has been the work of the "Gang of Four," Senators Rounds (R-SD), Heinrich (D-NM), Schumer (D-NY) and Young (R-IN). Following the second AI Forum, the Gang of Four introduced the Artificial Intelligence Advancement Act of 2023 (S. 3050), which would establish an artificial intelligence bug bounty program and require separate reports on: the use of AI platforms in financial services; vulnerabilities of AI-enabled military applications; and data sharing and coordination. Also following the AI Forum, Senators Schatz (D-HI) and Kennedy (R-LA) introduced the Schatz-Kennedy Labeling Act (S. 2691) to provide transparency around AI-generated content.

Another important milestone was the introduction of the bipartisan framework for AI legislation by Senators Blumenthal (D-CT) and Hawley (R-MO), who serve as the chair and ranking member, respectively, of the Senate Judiciary Subcommittee on Privacy, Technology and the Law. The bipartisan framework proposes a licensing regime targeting "sophisticated general-purpose AI models" to be administered by an independent oversight body. The framework also provides that Section 230 liability protections would not apply to AI and provides measures to promote transparency and protect children. Finally, the framework urges Congress to use export controls, sanctions and other restrictions to limit transfers of advanced AI models that can be used by foreign adversaries or used in human rights violations. The work of the senators and the Subcommittee has created critical momentum in this space, and the senators expect to produce draft text by the end of the year.

Legislative activity has spurred conversations around the benefits and risks of AI; however, Schumer has warned that Congress will likely not pass holistic legislation addressing AI until next year.

Pillsbury's multidisciplinary team of AI thought leaders and legal and strategic advisors is an industry leader in strategic promotion of responsible and beneficial AI. Pillsbury is closely monitoring AI-related legislative and regulatory efforts. Our AI team helps startups, global corporations and government agencies navigate the landscape impacted by emerging developments in AI. For insights on these rapidly evolving topics, please visit our Artificial Intelligence practice page.