KPMG

Regulatory Alert

Regulatory Insights

October 2023

Executive Order on Safe, Secure, and Trustworthy AI

Regulatory Insights:

- ***Broad coverage:*** *Covers principles of safety and security, privacy, civil rights, consumer and worker protections, innovation and competition, and national security. Emphasizes content labeling, watermarking, and transparency/reporting standards.*
- ***Multiple agency focus:*** *Pushes multiple federal agencies into regulation of AI risks affecting all industries.*
- ***More legislation and regulation:*** *Calls on Congress to pass data privacy legislation and calls for federal agencies to strengthen guidelines for data collection and privacy protections.*
- ***Regulatory Expectations:*** *Anticipate more rigorous standards/expectations from regulators around areas of data collection, testing, reporting, and outcomes. Expect needs for investments in tools and skills development for AI risk management and the use of AI to manage risk.*

The Administration issues an Executive Order (Order or EO) aimed at fostering the opportunities, and managing the risks, of artificial intelligence (AI), including Generative AI. The Order directs the establishment of new standards for AI safety and security, privacy protections, consumer and worker protections, and is intended to promote innovation and competition and advance equity and civil rights.

The Order builds on previous actions taken by the Administration, such as the publication of its AI Bill of Rights (see KPMG's Regulatory Alert, here), as well as efforts that resulted in voluntary commitments from fifteen (15) leading AI companies to "drive safe, secure, and trustworthy development of AI" (see White House announcement, here).

Highlights from the Order follow.

New Standards for AI Safety and Security

The Order directs federal agencies to implement comprehensive actions to protect against the potential risks of AI systems, including requiring:

- Developers of powerful AI systems (those that pose "serious risks to national security, national economic security, or national public health and safety") to notify the federal government when training a foundational model and to report "red team safety test" results and other critical information (under the Defense Production Act) to ensure the AI systems are safe, secure, and trustworthy before being made public.
- The National Institute of Standards and Technology (NIST) to set rigorous standards for extensive "red-team safety testing," and the Department of Homeland Security (DHS) to establish the AI Safety and Security Board to apply those standards to critical infrastructure sectors as well as to threats

from chemical, biological, radiological, nuclear, and cybersecurity risks.

- Agencies that fund life-science projects to establish new standards for biological synthesis screening to protect against the risks of AI in engineering dangerous biological materials.
- The Department of Commerce (DOC) to develop guidance for content authentication and watermarking to protect against AI-enabled fraud and deception.
- An advanced cybersecurity program for AI tools that builds on the Administration's ongoing AI Cyber Challenge and will be used to find and fix vulnerabilities in critical software.
- A National Security Memorandum to be developed by the National Security Council (NSC) and White House Chief of Staff, directing further actions on AI and security for military and intelligence community.

Privacy Protection

The Order emphasizes the need to protect Americans' privacy, particularly from risks posed by AI. Key actions include:

- Urging Congress to pass bipartisan data privacy legislation.
- Accelerating development and use of "privacy-preserving techniques," including ones that utilize advanced AI to train systems without compromising the privacy of the training data.
- Funding a Research Coordination Network to advance rapid breakthroughs and development of "privacy-preserving research and technologies" such as cryptographic tools, and to work with the National Science Foundation (NSF) promote their adoption by federal agencies.
- Focusing on evaluating agencies' collection and use of commercially available personal data and strengthening privacy guidance for federal agencies to account for AI-related risks.
- Developing guidelines for federal agencies to evaluate the effectiveness of privacy-preserving techniques, including those used in AI systems.

Innovation and Competition

The Order is intended to maintain and strengthen U.S. leadership in AI innovation and competition through actions including:

- Catalyzing AI research across the U.S. through a pilot of the National AI Research Resource (a tool that will provide AI researchers and students access to key AI resources and data) and expanded grants for AI research in areas such as healthcare and climate change.
- Promoting a "fair, open, and competitive" AI ecosystem by providing small developers and entrepreneurs access to technical assistance and resources, encouraging the Federal Trade Commission (FTC) to exercise its authorities, and helping small businesses commercialize AI breakthroughs.
- Modernizing and streamlining visa criteria, interviews, and reviews to expand opportunities for highly skilled immigrants and nonimmigrants with expertise in critical areas to study, stay, and work in the U.S.

Government Use of AI

To ensure responsible government deployment of AI and modernize federal AI infrastructure, the order directs agencies to:

- Issue guidance for agencies' use of AI, including clear standards to protect rights and safety, improve AI procurement, and strengthen AI deployment.
- Help agencies acquire specified AI products and services faster, more cheaply, and more effectively through more rapid and efficient contracting.
- Effect a government-wide AI talent surge by accelerating the rapid hiring of AI professionals and providing AI training for employees at all levels in relevant fields, to be led by the Office of Personnel Management (OPM), U.S. Digital Service, U.S. Digital Corps, and Presidential Innovation Fellowship.

Consumer, Patient, and Student Protection

The Order emphasizes the need to protect consumers, healthcare patients, and students from the risks of AI while ensuring AI's potential benefits. Among the directives:

- The Department of Health and Human Services (HHS) is to promote responsible use of AI in healthcare and drug development and to establish a

safety program to receive reports of unsafe AI practices.

— Resources should be created to shape the potential for deploying AI-enabled educational tools (e.g., personalized tutoring in schools).

Worker Protection

Addressing the impact of AI on jobs and workplaces, key directives include:

— Developing principles and best practices for mitigating the harms and maximizing the benefits of AI for workers, addressing job displacement, labor standards, workplace equity, health, safety, and data collection.

— Producing a report on AI's potential labor-market impacts and identifying options for strengthening federal support for workers facing labor disruptions, including from AI.

Equity and Civil Rights

To ensure AI advances equity and civil rights, the Order calls for actions including:

— Providing clear guidance to landlords, Federal benefits programs, and federal contractors to prevent AI algorithms from exacerbating discrimination.

— Addressing algorithmic discrimination through coordination with the Department of Justice (DOJ) and Federal civil rights offices develop training, technical assistance, and best practices, including investigating civil rights violations related to AI.

— Ensuring fairness in the criminal justice system by developing best practices in using AI for sentencing, parole, probation, pretrial release and detention, risk assessments, surveillance, crime forecasting, predictive policing, and forensic analysis.

International Efforts

The Order calls for continued collaboration with global partners to support safe, secure, and trustworthy deployment and use of AI worldwide. Key actions include:

— The State Department, in collaboration with DOC, leading an effort to establish robust international frameworks for collaboration on AI, ensuring safety and harnessing AI's benefits while managing risks.

— Accelerating development and implementation of vital AI standards with international partners and in standards organizations, ensuring that the technology is safe, secure, trustworthy, and interoperable.

— Promoting the safe, responsible, and rights-affirming development and deployment of AI abroad to solve global challenges (e.g., advancing sustainable development, mitigating dangers to critical infrastructure).

For more information, please contact Amy Matsuo, Matt Miller, or Bryan McGowan.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialme