

# Regulatory Alert

## Regulatory Insights

December 2023

### Landmark Actions Coming: The AI Act and Growing US Regulations

#### KPMG Insights:

- **Landmark Actions:** With the EU AI Act provisional agreement and the US Administration's Executive Order, landmark AI/GenAI regulatory actions will quickly necessitate robust and effective risk management and controls. Short-term impacts may include:
  - *Limitations/Prohibitions on Usage:* Certain uses of AI deemed 'unacceptable' could impact product or business strategies regarding planned usage or deployment of AI.
  - *Impact Assessments:* Required before certain 'high-risk' AI systems are put into the market, which could impact time to market for late-stage products.
- **Quick Pace:** The quick pace of regulatory and agency actions focuses on the development, use, disclosures/marketing and testing of AI/GenAI across several sectors (technology, defense, financial services and insurance, government), and in the US include multiple federal agencies (e.g., CISA, DOD, FCC, FTC, NAIC, NIST, OMB, and SEC).
- **What's Coming:** Expect further finalization of rulemaking to occur in the EU and other jurisdictions and in the US across federal agencies as additional deadlines from the U.S. Administration's Executive Order approach.

In the EU, the Council presidency and European Parliament reach provisional agreement on the AI Act (see releases [here](#) and [here](#)) including:

1. Risk-based clarification on high-impact and high-risk AI models and systems that may be deemed to cause systemic risk.
2. Revised governance and regulatory enforcement powers, including an AI Office within the Commission.
3. Technical documentation standards, including records of programming and training, adversarial testing, and measures taken to assess and mitigate risks for high-impact AI systems.
4. Bans on 'social scoring' and AI used to 'manipulate or exploit users'.

In the United States, recent AI/GenAI regulatory actions follow the Administration's October 2022 Blueprint for an Artificial Intelligence Bill of Rights and October 2023 Executive Order (EO) (14110) on safe, secure, and trustworthy AI (see KPMG's Regulatory Alerts, [here](#) and [here](#), respectively), as well as the National Institute for Standards and Technology's (NIST) release of its AI Risk Management Framework in January 2023. In recent months, Federal agencies have taken notable AI/GenAI regulatory actions. The table below (from August to December 2023) outlines the growing focus and breadth of regulatory coverage to drive safe, secure, and trustworthy AI/GenAI.

Agency	AI Topic	Type of Action	Description
CISA	Roadmap for AI	Guidance	Issues the <a href="#">2023 – 2024 Roadmap for Artificial Intelligence</a> , outlining its five lines of AI-related efforts, including: <ul style="list-style-type: none"> <li>— Responsible use of AI to support CISA mission (cyber defense).</li> <li>— Assure AI systems are secure and resilient by design through software development and implementation guidance.</li> <li>— Protect critical infrastructure from malicious use of AI.</li> <li>— Interagency, international, and public collaboration on AI efforts.</li> <li>— Expand AI expertise in CISA’s workforce.</li> </ul>
	Joint Guidelines for AI Development	Guidance	With the United Kingdom’s National Cyber Security Centre (NCSC), releases joint <a href="#">Guidelines for Secure AI System Development</a> to help developers of any systems that use AI make informed cybersecurity decisions at every stage of the development process, including design, development, deployment, and operation and maintenance.
DOD	AI-related Efforts	Testing, Development, Integration	Prior to the issuance of the Administration’s EO, the following initiatives related to AI had already been established: <ul style="list-style-type: none"> <li>— In August 2023, DOD established a <a href="#">GenAI task force</a>, led by the Chief Digital and Artificial Intelligence Office (CDAO), to assess, synchronize, and employ GenAI capabilities across the DOD.</li> <li>— In September 2023, DOD established two <a href="#">AI “Battle Labs”</a> at U.S. European Command and U.S. Indo-Pacific Command, in collaboration with CDAO’s Algorithmic Warfare Directorate and the Defense Innovation Unit, to expedite learning from DOD operational theater data (logistics, cyber, telemetry).</li> <li>— In September 2023, DOD’s National Security Agency (NSA) announced the creation of an <a href="#">AI Security Center</a> to oversee the development and integration of AI capabilities within U.S. national security systems, including best practices, evaluation methodologies, and risk frameworks.</li> </ul>
FCC	AI Calling Initiative	Information Collection	<a href="#">Notice of Inquiry</a> focuses on the use of AI technologies in “unwanted and illegal telephone calls and text messages under the Telephone Consumer Protection Act (TCPA)” and seeks to gather information to define AI under TCPA, consider potential liability for AI developers who design systems that violate TCPA, and understand AI’s potential risks and benefits in the telecommunications sector.
FTC	Compulsory Process for AI Products/ Services	Administrative Process	Approves a resolution authorizing the use of <a href="#">compulsory process</a> in nonpublic investigations involving products and services that use or claim to be produced using AI or claim to detect its use. The authorization is intended to streamline FTC staff’s ability to issue civil investigative demands (CIDs), which are a form of compulsory process similar to a subpoena, in investigations.
	AI Voice Cloning	Testing, Information Collection	<a href="#">Voice Cloning Challenge</a> is intended to address “the present and emerging harms of AI or AI-enabled voice cloning technologies” and focuses on the potential risks and benefits of AI voice cloning technologies under the FTC Act, the Telemarketing Sales Rule, as well as the proposed Impersonation Rule. The rules for the challenge require

			that submissions address at least one of three “intervention points”: 1) prevention or authentication, 2) real time detection or monitoring, or 3) post-use evaluation.
<b>NAIC</b>	Model Bulletin on Use of AI by Insurers	Guidance	Membership adopts the <a href="#">Model Bulletin on the Use of Artificial Intelligence Systems by Insurers</a> , which is to guide and foster uniformity among state insurance regulators regarding expectations for insurance carriers deploying AI. The bulletin emphasizes the importance of responsible governance, risk management policies, and procedures to ensure fair and accurate outcomes for consumers.
<b>NIST (DOC)</b>	U.S. AI Safety Institute & Consortium	Announcement	Establishes the <a href="#">U.S. Artificial Intelligence Safety Institute</a> (USAISI) and a related consortium (comprised of organizations with technical, product, data, and/or model expertise) dedicated to equipping and empowering the “collaborative establishment of a new measurement science that will enable the identification of proven, scalable, and interoperable techniques and metrics to promote development and responsible use of safe and trustworthy AI.”
<b>OCC</b>	Semi-Annual Risk Perspective Report	Report	Publishes the Fall 2023 edition of its <a href="#">Semiannual Risk Perspectives Report</a> highlighting its view on key risks and issues facing the federal banking system. The report identifies AI and GenAI technologies as an “emerging risk” based on banks’ increasing utilization of these technologies for various risk management and operational purposes, posing challenges in areas such as compliance, credit, reputational, and operational risk, (e.g., potential bias, privacy concerns, and errors/fraud). Banks are expected to “manage AI use in a safe, sound, and fair manner, commensurate with the materiality and complexity of the particular risk of the activity.”
<b>OMB</b>	EO Implementation Guidance	Draft Guidance	In response to the Administration’s EO, releases draft <a href="#">implementation guidance</a> that would require federal agencies to: <ul style="list-style-type: none"> <li>— Establish AI governance structures in federal agencies (Chief AI Officer (CAIO)).</li> <li>— Advance responsible AI innovation through enterprise AI strategies.</li> <li>— Manage risks from government uses of AI.</li> </ul>
<b>SEC</b>	“AI-Washing”	Remarks	In <a href="#">remarks</a> to a conference audience, the SEC Chair warns businesses against “AI-washing” or making false artificial intelligence-related claims, comparing it to “greenwashing” or overstating environmental or climate-related records. “Greenwashing” has been a priority of agency examinations and enforcement actions, as has the focus on fund names that suggest focus on environmental, social, or governance (ESG) factors.
	Reliance on GenAI	Remarks	In <a href="#">remarks</a> at an AI Summit, the SEC Chair warns that too many financial services firms relying on too few GenAI models for processes (e.g., trading, underwriting, etc.) could result in the potential emergence of a “monoculture” or a flash crash of the markets.
	“Covered Technologies” and Conflicts of Interest	Proposal	Issues proposed rules (see KPMG’s Regulatory Alert, <a href="#">here</a> ) under the Securities Exchange Act and the Investment Advisers Act that would seek “to eliminate, or neutralize the effect of, conflicts of interest associated with broker-dealers’ or investment advisers’ interactions with investors through the use of technologies that optimize for, predict, guide, forecast, or direct, investment-related behaviors or outcomes.”

For more information, please contact [Amy Matsuo](#) or [Bryan McGowan](#).

## Contact the author:



**Amy Matsuo**  
**Principal and National Leader**  
Regulatory Insights  
[amatsuo@kpmg.com](mailto:amatsuo@kpmg.com)

[kpmg.com/socialme](https://kpmg.com/socialme)



**Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.**

All information provided here is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the facts of the particular situation. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.