



AI Regulations: Present & Future

Present Regulatory Trajectories
and Future Horizons

April 2024

Table of Contents

<u>Key Takeaways</u>	2
<u>Alignment on Regulatory Principles</u>	3
<u>AI Regulatory Frameworks</u>	4
<u>More Regulatory Actions Coming</u>	5
<u>Need for AI Governance Action</u>	18
<u>Relevant Thought Leadership</u>	19



The regulatory principles of fairness, explainability, data integrity, security and resiliency, accountability, privacy, and risk management transcend regulatory issuances, in the US and globally. Regulators will use existing rules and authorities as well as continue to issue both continued regulatory frameworks... and increasingly regulatory enforcement. The time for simply establishing sound risk governance and risk management AI programs is quickly passing – the time for implementing, operationalizing, demonstrating and sustaining effective risk practices is now.

Amy Matsuo

Principal
U.S. Regulatory Insights Leader
KPMG LLP



With continued global and US regulation on the horizon, now is the time for U.S. businesses to implement Trusted AI programs to quickly assess and understand risks and exposures. Organizations must move from planning to operationalizing ethical principles into practice and institute responsible governance, policies and controls aligned to leading frameworks and emerging regulations. Responsible and ethical AI must be embedded by design across the AI lifecycle.

Bryan McGowan

Partner
U.S. Trusted AI Leader
KPMG LLP

Key Takeaways



What can business expect in both AI regulations and regulatory focus?

While the US will continue to see more fragmented approaches, the regulators have quickly aligned on core regulatory principles as well as confirmation to the market that current regulations will apply to the use of AI.

Businesses should expect:

1

Alignment on Regulatory Principles

Fairness, explainability/accountability, risk management, security and resiliency, data privacy, data integrity

2

Use/Expansion of AI Regulatory Frameworks

Evolving cyber and risk management frameworks and expanded use for existing model risk and third-party frameworks

3

More Regulatory Actions Coming

Increasing regulatory questions re: AI and regulatory enforcements (using existing regulations)

4

Need for AI Governance Action

Heightened regulatory expectations for companies to implement an AI governance framework with appropriate controls, documentation, monitoring, testing, and management/Board oversight

Alignment on Regulatory Principles

1

2

3

4

Across agencies, regulators are aligning on foundational principles to supervise and enforce responsible development and deployment of AI.



Fairness

Ensuring fairness in applications of AI and other innovative technologies by mitigating risks of bias/consumer harm; subjecting models/uses to ongoing testing and oversight



Explainability/Accountability

- Demonstrable AI explainability (transparency) and accountability from the Board and model developers
- Content authentication and “watermarking”



Risk Management

- Risk management and governance around the design, use, and deployment of AI, including:
- Robust AI development, implementation, and use (e.g., Clear statement of purpose; sound design/theory/logic)
 - Effective validation conducted independently of the AI design and development
 - Sound governance, policies, and controls



Security & Resiliency

- Models meet their intended use and contain protections against unintended use, including adversarial attacks, data poisoning, insider threat, model reverse engineering.
- Testing using established standards prior to public release
- Improving resiliency, and preventing critical disruptions



Data Privacy

Limitations on access to and use of consumer data for specific, and/or explicit purposes, subject to permission, consent, opt in/out, and/or authorization, as required



Data Integrity

Ensuring accuracy, consistency, and validity of data used in the design and application of technological tools

AI Regulatory Frameworks

1

2

3

4

In keeping with the Administration’s October 2023 Executive Order on Safe, Secure, and Trustworthy AI (EO 14110), federal agencies are looking to utilize existing and create new frameworks to both better understand and supervise the widespread use of AI. Frameworks look to address the core regulatory principles of AI and regulators’ expectations are likely to include processes/elements for:



Fairness



Explainability/
Accountability



Risk
Management



Security &
Resiliency



Data Privacy



Data Integrity

Risk Governance

Culture of Accountability

Managing Risk

Continual Improvement

- ❖ Governing, mapping, measuring and managing AI risks
- ❖ Understanding the inter-relationships among the principles (i.e., trustworthiness characteristics), changing societal dynamics/human behavior (“socio-technical approaches”), and AI risk
- ❖ Making go/no-go system commissioning and deployment decisions
- ❖ Promoting accountability related to AI system risks
- ❖ Striving for a corporate culture that prioritizes the identification and management of AI system risks and potential impacts to individuals, communities, organizations, and society
- ❖ Assessing potential downstream risks (e.g., safety, bias, influence over decisions of policy makers)
- ❖ Augmenting capacity for testing, evaluating, verifying, and validating (TEVV) AI systems and associated risks
- ❖ Information sharing within and across organizations and regulators regarding risks, decision-making processes, responsibilities, common pitfalls, TEVV practices, and approaches for continual improvement

More Regulatory Actions Coming: Federal





1

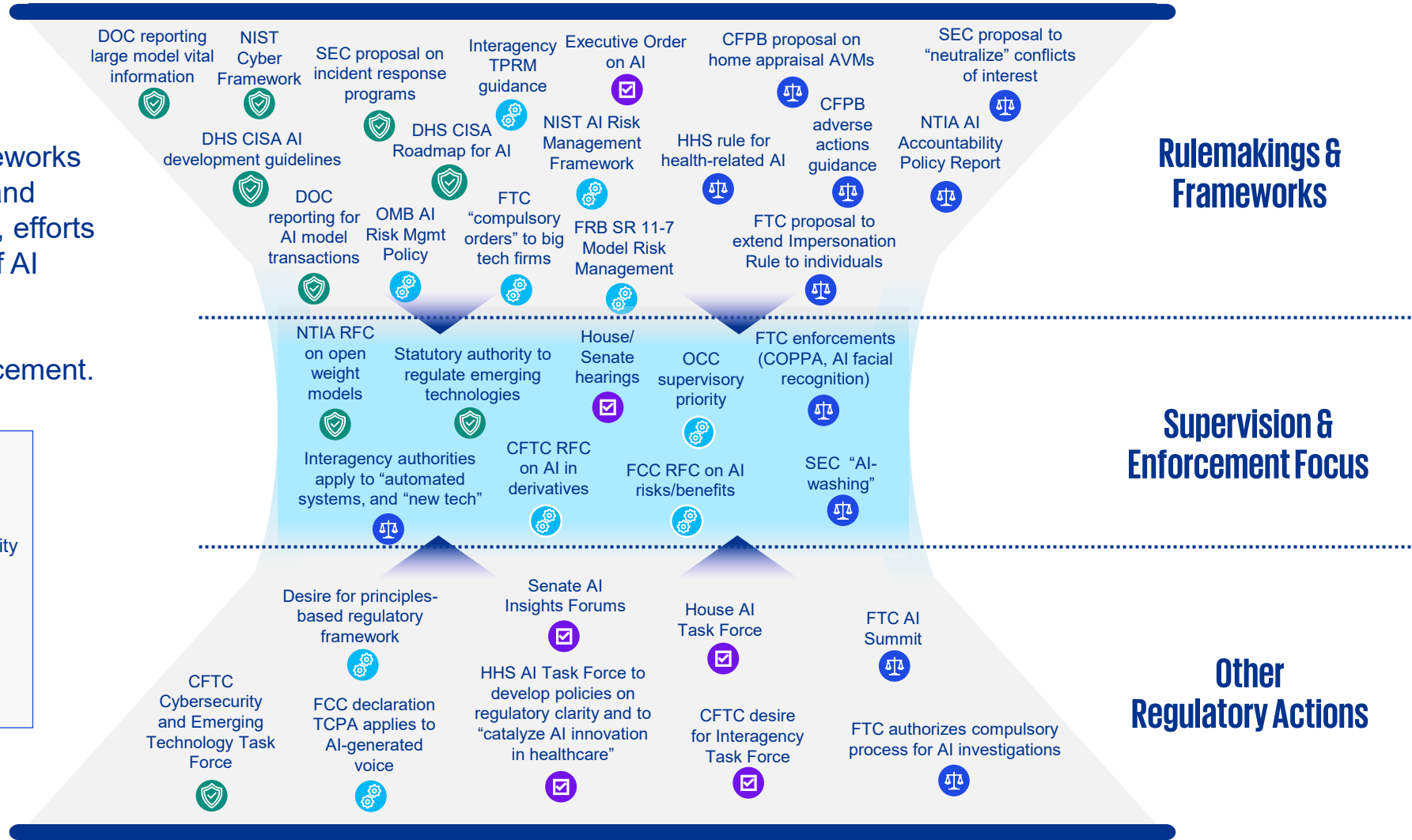
2

3

4

Rulemaking and frameworks will drive supervision and enforcement. Similarly, efforts to further discussion of AI risks/benefits will drive policies that impact supervision and enforcement.

-  All AI Principles
-  Fairness
Explainability/Accountability
-  Risk Management
-  Security & Resiliency
Data Privacy
Data Integrity



Rulemakings & Frameworks

Supervision & Enforcement Focus

Other Regulatory Actions

More Regulatory Actions Coming: Federal

1

2

3

4

AI-related regulatory activities continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing authorities, regulations, and frameworks can (and will) be applied to AI. Examples of recent regulatory activities across U.S. federal agencies include:



White House



U.S. Congress



Department of Commerce



Federal Trade Commission



Securities and Exchange Commission



Commodity Futures Trading Commission



Federal Reserve Board



Federal Deposit Insurance Corporation



Office of the Comptroller of the Currency



Consumer Financial Protection Bureau



Federal Communications Commission



Department of Health and Human Services



Cybersecurity and Infrastructure Security Agency

[Click each agency below to learn more.](#)

More Regulatory Actions Coming- Federal

1

2

3

4



AI regulatory actions continue to expand via proposed rules, requests for information/comment, guidance, and notices. At the same time, regulators continue to reiterate that their existing rules and regulations can (and will) be applied to AI. Examples of AI-related actions include:



Executive Order

Calls for a “whole of government” approach to establish safe, secure, and trustworthy AI emphasizing transparency and accountability in AI development and deployment and directs federal agencies to prioritize AI technologies that promote economic growth and job creation while minimizing potential negative impacts on workers and communities. The EO follows the Administration’s Blueprint for an AI Bill of Rights, a set of principles and practices to guide the design, use, and deployment of automated systems to protect the public.

White House



Framework

OMB government-wide AI risk management policy requiring federal agencies to implement safeguards when using AI in a manner that impacts the safety or rights of Americans by December 1, 2024.



Task Force

- ❖ House establishes Task Force on Artificial Intelligence to develop guiding principles, recommendations, and policy proposals addressing innovation, competition, national security, and guardrails/protections.
- ❖ Senate AI working group conducts a series of AI Insights Forums to serve as the basis of a report and future AI legislation.

U.S. Congress

Hearings

House and Senate hearings being convened across multiple committees, including Judiciary, Commerce, Financial Services, Intelligence

House
Senate



Fairness



**Explainability/
Accountability**



**Risk
Management**



**Security &
Resiliency**



Data Privacy



Data Integrity



Cybersecurity and Infrastructure Security Agency

More Regulatory Actions Coming- Federal

1

2

3

4



AI regulatory activities continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing authorities and regulations can (and will) address AI risks.

Click each agency seal below to learn more.

Framework

- ❖ NIST AI Risk Management Framework, plus RFC on guidelines for evaluating AI technologies, red-teaming tests, and AI capabilities (benchmarks)
- ❖ NIST Cybersecurity Framework
- ❖ NTIA AI Accountability Policy Report

Reporting

Require developers of the “most powerful” AI systems (including potential “dual-use foundation models”) to report vital information, especially AI safety test results.

Proposed Rule

Proposal to require cloud services providers (providing Infrastructure as a Service) to report certain transactions with foreign customers involving large AI models (e.g., “dual use foundational models”) that may aid national security-related “cyber-enabled activity” such a denial-of-service attacks.

Request for Comment

NTIA RFC on risks, benefits, and potential policy related to advanced AI models with widely-available model weights



Department of Commerce

NIST
NTIA



Federal Trade Commission



Securities and Exchange Commission



Fairness



Explainability/ Accountability



Risk Management



Security & Resiliency



Data Privacy



Data Integrity



Cybersecurity and Infrastructure Security Agency

More Regulatory Actions Coming: Federal

1

2

3

4



AI regulatory activities continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing authorities and regulations can (and will) be applied to AI. Examples of recent regulatory activities across U.S. federal agencies include:



Inquiry

Extend “compulsory orders” to five big tech firms to report recent partnerships and investments with AI companies and major cloud service providers to gain understanding of market trends, business practices, and impact to competition.

Click each agency seal below to learn more.

Proposed Rule

Proposal to extend the Impersonation Rule to individuals, including protections against AI-generated “deepfakes”.

Summit

AI Summit to discuss key developments in AI, including infrastructure requirements, data and model issues, and impacts on consumers and competition.

Other Actions

- ❖ Authorizes compulsory process for AI-related investigations
- ❖ Enforcement actions relating to COPPA and AI facial recognition



Fairness



Explainability/
Accountability



Risk
Management



Security &
Resiliency



Data Privacy



Data Integrity

Cybersecurity and Infrastructure Security Agency

More Regulatory Actions Coming: Federal

1



2

3

4



AI regulatory activities continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing authorities and regulations can (and will) be applied to AI. Examples of recent regulatory activities across U.S. federal agencies include:

 <p>SEC Securities and Exchange Commission</p>	<p>Proposed Rule</p>	<p>Proposal to “neutralize” conflicts of interest associated with the use of predictive analytic technologies, including AI.</p> <p>Agency seal below to learn more.</p>
<p>SEC Securities and Exchange Commission</p>	<p>Proposed Rule</p>	<p>Proposal to amend Regulation S-P to require adoption of incident response programs including procedures to notify impacted individuals.</p>
 <p>FTC Federal Trade Commission</p>	<p>Supervision</p>	<ul style="list-style-type: none"> ❖ Focus on “AI-washing”—making false or misleading claims about the use of AI models/tools—with related enforcement actions under the Marketing Rule. ❖ Division of Enforcement Director calls out “perfect storm or risk” brewing around AI, given high investor and market interest; reiterates need for representations that are not false or misleading.



Fairness



Explainability/
Accountability



Risk
Management



Security &
Resiliency



Data Privacy



Data Integrity

CISA **Cybersecurity and Infrastructure Security Agency**

More Regulatory Actions Coming: Federal

1

2

3

4



AI regulatory activities continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing authorities and regulations can (and will) be applied to AI. Examples of recent regulatory activities across U.S. federal agencies include:

Request for Comment

RFC on the current and potential uses of AI in CFTC-regulated derivatives markets and the implications of such use/adoption, including risk mitigation. Areas of interest include trading, data processing and analytics, risk management, compliance, books and records, systems development, cybersecurity and resilience, and customer interactions.

Click each agency seal below to learn more.

CFTC
Commodity
Futures Trading
Commission

Task Force

- ❖ Establish Cybersecurity and Emerging Technology Task Force to address cybersecurity-related issues including data protection, system safeguards, market manipulation, potential role of AI in compliance violations, and risk management.
- ❖ Desire to create an inter-agency task force (CFTC, SEC, FRB, OCC, CFPB, FDIC, FHFA, NCUA) to support the AI Safety Institute development of guidelines, tools, benchmarks and best practices for use and regulation of AI in financial services.



Cybersecurity and Infrastructure Security Agency

More Regulatory Actions Coming- Federal

1

2

3

4



AI regulatory actions continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing rules and regulations can (and will) address the risks of AI.

FRB

Federal Reserve Board

Framework

- ❖ Model Risk Management (FRB SR 11-7) covering model development, implementation and use; model validation; and governance, policies, and controls.
- ❖ Third-Party Risk Management (Joint Guidance) covering all stages in the life-cycle of third-party relationships.
- ❖ Desire a principles-based regulatory framework

Click each agency seal to learn more.

FDIC

Federal Deposit Insurance Corporation

Supervision

Individually and collectively state they have statutory authority to regulate emerging technologies and that they will hold institutions accountable for the use of new technologies consistent with the expectations in existing model risk management guidance.

OCC

Office of the Comptroller of the Currency

Supervision

OCC identifies AI as a supervisory priority, directing examiners to “identify and assess products, services, and third-party relationships with unique, innovative, or complex structures” such as AI technologies with a focus on risk management and governance, monitoring, and talent.



More Regulatory Actions Coming: Federal

1

2

3

4



AI regulatory activities continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing authorities and regulations can (and will) be applied to AI. Examples of recent regulatory activities across U.S. federal agencies include:

Supervision
 Joins DOJ, EEOC, FTC in stating their existing legal authorities apply to the use of “automated systems” and “innovative new technologies” just as they apply to other practices. They express concern over data and datasets, model opacity and access, and design and use, and will enforce anti-discrimination, civil rights, fair competition, and consumer protection laws.

Guidance
 Requires lenders to provide “specific and accurate reasons when taking adverse actions against consumers” including when decisions are made using complex algorithms such as AI or “other predictive decision-making technologies”.

Proposed Rule
 Proposal, jointly with FRB, OCC, FDIC, NCUA, FHFA, to establish standards to mitigate risks associated with automated valuation models used in home appraisals.



Consumer Financial Protection Bureau



Fairness



Explainability/ Accountability



Risk Management



Security & Resiliency



Data Privacy



Data Integrity

More Regulatory Actions Coming: Federal

1

2

3

4



AI regulatory activities continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing authorities and regulations can (and will) be applied to AI. Examples of recent regulatory activities across U.S. federal agencies include:

Click each agency seal below to learn more.



Federal Communications Commission

Request for Comment

Seeks comment to better understand potential AI risks and benefits to telecommunications (including telephone and text messages), including protections under the Telephone Consumer Protection Act (TCPA).

Declaration

Confirms that the TCPA applies to AI technologies that generate human voices; calls made with AI-generated voices are “artificial” and require the prior express consent of the called party.



Fairness



Explainability/ Accountability



Risk Management



Security & Resiliency



Data Privacy



Data Integrity



Cybersecurity and Infrastructure Security Agency

More Regulatory Actions Coming: Federal

1

2

3

4



AI regulatory actions continue to expand via proposed rules, requests for information/comment, guidance, and speeches. At the same time, regulators continue to reiterate that their existing laws and regulations can (and will) be applied to AI. Examples of recent regulatory activities across U.S. federal agencies include:

HHS

Department of Health and Human Services

Final Rule

Rulemaking, through HHS ONC (Office of National Coordinator for Health Information Technology), establishing new and revised health IT certification requirements/standards related to AI and other predictive algorithms to increase transparency and promote fairness in health records.

Task Force

HHS AI task force to develop policies providing regulatory clarity and “catalyze AI innovation in healthcare”.

CISA

Cybersecurity and Infrastructure Security Agency

Guidance

- ❖ DHS CISA Roadmap for AI – building on CISA’s cybersecurity and risk management programs, intended to promote “security by design”, including transparency, accountability, and security
- ❖ DHS CISA and UK Joint Guidelines for Secure AI System Development covering the full development lifecycle.



Fairness



Explainability/ Accountability



Risk Management



Security & Resiliency



Data Privacy



Data Integrity

Cybersecurity and Infrastructure Security Agency

More Regulatory Actions: State

1

2

3

4

States are addressing AI through both legislation and regulation. Select State activity includes:

Utah

Artificial Intelligence Policy Act:

Consumer protection law effective May 1, 2024, requiring entities and individuals using AI/Gen AI to disclose use of such tools when interacting with customers (establishing liability for inadequate/improper disclosure). Also creates an Office of AI Policy and a regulatory AI analysis program.

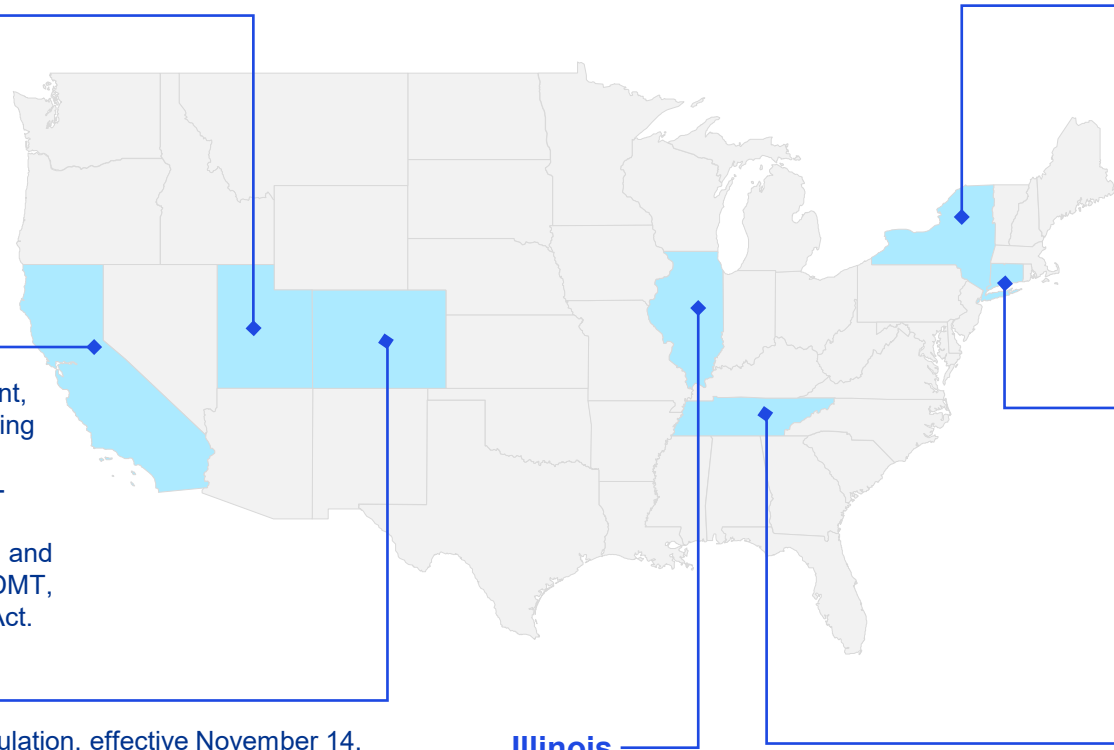
California

Executive Order: Directing study of development, use, and risks of AI; develop process for evaluating and deploying AI within state government.

CPPA: Draft regulations for automated decision-making technology (ADMT) including AI, which would provide for consumers rights to opt out of, and access information about, businesses' use of ADMT, as outlined in the California Consumer Privacy Act. A formal proposed rule is still forthcoming.

Colorado

Colorado Division of Insurance: A new AI regulation, effective November 14, 2023, requires licensed life insurance companies that use external consumer data and information sources (ECDIS) and/or algorithms and predictive models to establish a risk-based governance and risk management framework to mitigate the risk of unfair discrimination based on race and remediate unfair discrimination, if detected. Reporting requirements include a compliance progress report on June 1, 2024, and an annual compliance attestation beginning December 1, 2024.



New York

NY DFS: Proposed guidance on the use of AI by insurers, including expectations for developing and managing the integration of external consumer data and information sources (ECDIS), AI systems, and other predictive models to mitigate potential consumer harm; covers anti-discrimination and risk management/governance framework.

NYC: Law requiring AI and automated employment decision tools to be audited for bias and disclosed to prospective candidates/employees.

Connecticut

OLR Public Act Concerning AI, Automated Decision Making, and Personal Data Privacy: Requires the Department of Administrative Services to inventory all systems employing AI being used by state agencies. Effective February 1, 2024, the department must also conduct ongoing assessments of such systems to mitigate risk of discrimination or disparate impact.

Illinois

Artificial Intelligence Video Interview Act, effective 2020, governs the use of AI on video interviews, including requirements for disclosure, consent, confidentiality, and deletion.

Tennessee

ELVIS Act, effective July 1, 2024, adds “voice” (actual or simulation) to personal property rights of name, image, and likeness and adds protections against their unauthorized use in any medium and in any manner.

More Regulatory Actions: International

1

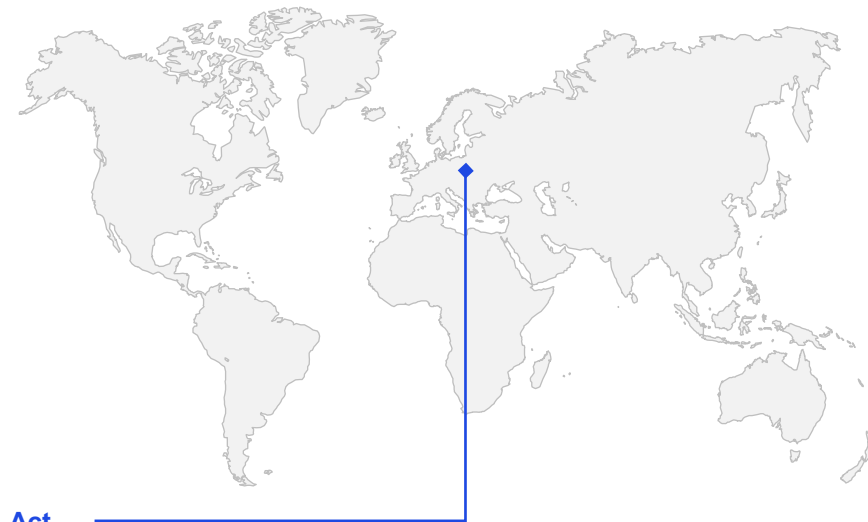
2

3

4

International Activity, including:

Concurrent with efforts in the U.S., AI-related laws, regulations, and frameworks are being introduced and implemented globally (e.g., Singapore, China, Brazil, EU, OECD), some of which have far reaching impacts (notably the EU AI Act, outlined below). These actions touch on a variety of areas, such as privacy, consumer protection, data security, intellectual property, product liability, and competition and may/will impact U.S. companies' product and/or business strategies with regard to planned usage or deployment of AI.



EU AI Act

The EU Artificial Intelligence Act establishes a regulatory framework for the development and use of AI that prioritizes safety, transparency, and accountability. The EU AI Act sets out strict requirements for AI developers and users, including mandatory risk assessments and transparency obligations/documentation requirements. It also establishes a European Artificial Intelligence Board to oversee the implementation of the Act and provide guidance on AI-related issues. U.S. multi-national corporations with operations in the EU that meet the criteria of the regulation will be required to comply.

Need for AI Governance Action

1

2

3

4

As we await potential legislation from the U.S. Congress and/or new final rulemakings from federal agencies, organizations can proactively prepare with these actions:

Short-term:

Define the appropriate governance

- ❖ Implement your AI governance framework
- ❖ Define policy to identify risk levels for AI systems
- ❖ Manage stakeholder expectation
- ❖ Set up sustainable data management practices

Know your risks

- ❖ Prioritize and manage AI risks
- ❖ Perform inventory and classify current AI landscape
- ❖ Conduct a gap analysis
- ❖ Test AI systems
- ❖ Define third party risk management process

Initiate a scalable approach

- ❖ Document and maintain records
- ❖ Automate system management and evaluation
- ❖ Train employees on AI ethics and compliance
- ❖ Establish usage guidelines

Mid- to long-term:

Anticipate Regulatory impacts on business processes

- ❖ Build consumer trust through transparency.
- ❖ Align strategically with regulatory changes
- ❖ Collaborate and keep an open dialogue with industry and policy makers.

Develop Ethics & Governance

- ❖ Prioritize long-term investment in AI ethics and governance.
- ❖ Maintain ongoing AI literacy and training programs

Embed trusted AI in innovation, design and control

- ❖ Innovate within ethical boundaries
- ❖ Implement trusted AI and security by design
- ❖ Audit and update the AI system regularly

Relevant Thought Leadership

From KPMG Regulatory Insights



- ❖ [AI Regulation: Cross-Agency Actions](#)
- ❖ [Enforcement/Supervision to “Automated Systems”](#)
- ❖ [Ensuring Trust in AI: Commerce Department Request for Comment](#)

From KPMG Firmwide



[KPMG Speed to Modern Technology: Responsible AI](#)



[Download the paper](#)



[Download the paper](#)

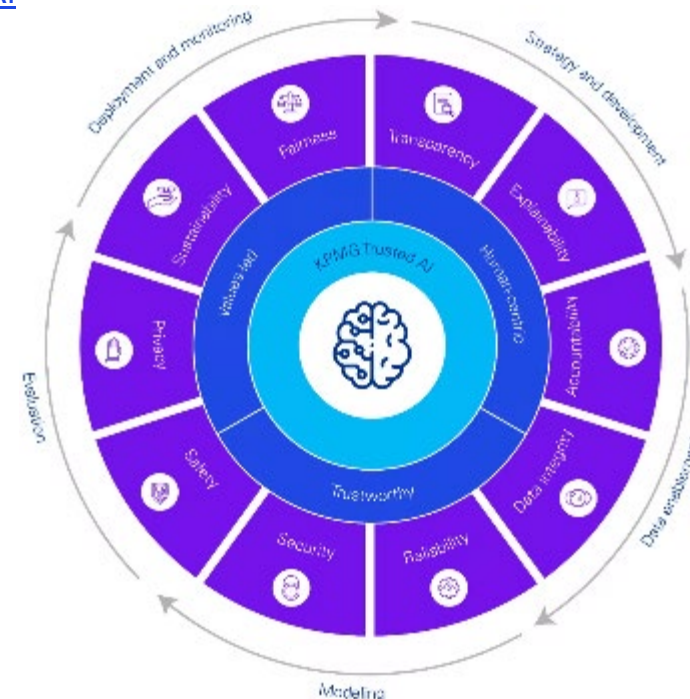


[Download the paper](#)

KPMG Trusted AI Approach

Implementing trustworthy and ethical AI is a complex business, regulatory, and technical challenge. KPMG Trusted AI is our strategic approach and framework to designing, building, deploying and using AI solutions in a responsible and ethical manner. It was developed based on the combination of our extensive experience in AI risk management and input from existing global standards.

[KPMG Trusted AI](#)





Contact us



Amy Matsuo
Principal
U.S. Regulatory Insights Leader
amatsuo@kpmg.com



Bryan McGowan
Principal
U.S. Trusted AI Leader
bmcgowan@kpmg.com



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



kpmg.com/socialmedia

The information contained herein 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 particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP483563-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.