Compliance Today - March 2024

Nakis Urfi (nakis.urfi@nakis.urfi, linkedin.com/in/nurfi/) is a Senior Manager, Provider Relations & Regulatory Compliance at Abbott based in Dallas, TX.

Navigating new frontiers: Review of the AI Executive order and OMB federal agency guidance

by Nakis Urfi

The United States has been lagging in substantive artificial intelligence (AI) legislation compared to the rest of the world. The EU agreed on the terms of the AI Act, touting that "fundamental rights, democracy, the rule of law and environmental sustainability are protected from high-risk AI, while boosting innovation and making Europe a leader in the field."[1]

Many other countries have substantive proposed AI regulations under consideration.[2] Even the U.S' self-acknowledged technological competitor, China,[3] has far-reaching regulations in place already for algorithms, generative AI, and ethical reviews of science and technology activities.[4]

There is an argument that the U.S. has purposely been delaying federal regulations to continue to allow for rapid innovation and commercialization of AI development. However, such an approach poses fundamental risks to the American people; it begs the question of how long we want to subject ourselves to take such broad risks that can come with an ever-growing list of potentially harmful outcomes, including the usage of "dark AI," which is the concept of programming AI intentionally or unintentionally to carry out malicious activities.

Enter the Executive order on the Safe, Secure, and Trustworthy Development and Use[5]

In October 2023, President Joe Biden issued a landmark Executive order (EO) establishing new standards for AI safety and security, protecting Americans' privacy, advancing equity and civil rights, standing up for consumers and workers, and promoting innovation and competition.

The EO makes clear that managing AI risks will be a main priority moving forward, and the following are some highlights.

New standards for AI safety and security

- Require developers of the most powerful AI systems share their safety test results and other critical information with the U.S. government. The EO will require companies developing any foundation model that poses a serious risk to national security, national economic security, or national public health and safety must notify the federal government and share the results of all red-team safety tests.
- Develop standards, tools, and tests to help ensure that AI systems are safe, secure, and trustworthy. The

National Institute of Standards and Technology will set rigorous standards for extensive red-team testing to ensure safety before public release.

- Protect against the risks of using AI to engineer dangerous biological materials by developing new standards for biological synthesis screening. Agencies that fund life–science projects will establish these standards as a condition of federal funding, creating incentives to ensure adequate screening and manage risks potentially made worse by AI.
- Protect Americans from AI-enabled fraud and deception by establishing standards and best practices for detecting AI-generated and authenticating official content. The U.S. Department of Commerce will develop guidance for content authentication and watermarking to clearly label AI-generated content.
- Establish an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software, building on the Biden–Harris administration's ongoing "AI Cyber Challenge."

Protecting Americans' privacy

- President Biden calls on Congress to pass bipartisan data privacy legislation to protect all Americans—especially kids.
- Protect Americans' privacy by prioritizing federal support for accelerating the development and use of privacy-preserving techniques.
- Evaluate how agencies collect and use commercially available information—including information they procure from data brokers—and strengthen privacy guidance for federal agencies to account for AI risks.
- Develop guidelines for federal agencies to evaluate the effectiveness of privacy-preserving techniques, including those used in AI systems.

Advancing equity and civil rights

- Provide clear guidance to landlords, federal benefits programs, and federal contractors to keep AI algorithms from being used to amplify discrimination.
- Address algorithmic discrimination through training, technical assistance, and coordination between the U.S. Department of Justice and federal civil rights offices on best practices for investigating and prosecuting AI civil rights violations.

Standing up for consumers, patients, and students

- Advance the responsible use of AI in healthcare and the development of affordable and life-saving drugs. The U.S. Department of Health and Human Services (HHS) will also establish a safety program to receive reports of—and act to remedy—harms or unsafe healthcare practices involving AI.

Other noteworthy aspects of the EO

- Develop principles and best practices to mitigate the harms and maximize the benefits of AI for workers.
- Promoting innovation and competition through providing more resources for research and pushing for a fair, open, and competitive AI ecosystem.
- Continue working with other nations to support safe, secure, and trustworthy deployment and use of AI

worldwide, including multistakeholder engagements, and accelerate the development of AI standards.

- Propose regulations that require U.S. Infrastructure as a Service (IaaS) providers to submit a report when a foreign person transacts with that IaaS provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity.
- Include appropriate personnel dedicated to collecting and analyzing AI-related intellectual property (IP) theft reports.
- Establish an HHS AI task force that "shall, within 365 days" of its creation, develop a strategic plan that includes policies and frameworks—possibly including regulatory action, as appropriate—on responsible deployment and use of AI and AI-enabled technologies in the HHS sector.

It is apparent that the U.S. is now driving toward pushing for stronger oversight of AI development with clearer objectives and guardrails. This includes pushing to mitigate risks from generative AI and overall AI uses, creating more AI governance structures, training staff on AI impacts, protecting privacy, addressing bias, and preparing the U.S. for broader international implications with cybersecurity and IP risks.

Enter the White House OMB draft memorandum to federal agencies [6]

Following the EO, the Office of Management and Budget (OMB) released a draft policy on "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" in November 2023. This guidance establishes AI governance structures in federal agencies, advances responsible AI innovation, increases transparency, protects federal workers, and manages risks from government uses of AI.

Here are some of the OMB's policy highlights.

Increase AI governance

- Designate chief AI officers who would advise agency leadership on AI, coordinate and track the agency's AI activities and advance AI use in the agency's mission, and oversee the management of AI risks. The role, responsibilities, and reporting structure are stated in the memo.
- Establish AI governance boards to establish internal mechanisms for coordinating the efforts of AI issues. It is stated who should chair the board and the levels of representation that should be included.
- Expand reporting on AI use cases, including providing additional detail on AI systems' risks and how the agency is managing those risks.
- Publish online plans for the agency's compliance with the guidance, including aligning internal AI principles and guidelines with this memo.

Advancing responsible AI innovation

- Develop an agency AI strategy, covering areas for future investment as well as plans to improve the agency's enterprise AI infrastructure, its AI workforce, capacity to successfully develop and use AI, and ability to govern AI and manage its risks.
- Remove unnecessary barriers to the responsible use of AI, including those related to insufficient information technology infrastructure, inadequate data and data sharing, gaps in the agency's AI workforce and workforce practices, and cybersecurity approval processes poorly suited to AI systems.

- Explore the use of generative AI in the agency, with adequate safeguards and oversight mechanisms.

Managing risks from the use of AI

- Mandate the implementation of specific safeguards for uses of AI that impact the rights and safety of the public. These safeguards include conducting AI impact assessments and independent evaluations; testing the AI in a real-world context; identifying and mitigating factors contributing to algorithmic discrimination and disparate impacts; monitoring deployed AI; sufficiently training AI operators; ensuring that AI advances equity, dignity, and fairness; consulting with affected groups and incorporating their feedback; notifying and consulting with the public about the use of AI and their plans to achieve consistency with the proposed policy; notifying individuals potentially harmed by use of AI and offering avenues for remedy; and more.
- Define uses of AI that are presumed to impact rights and safety, including many uses involved in health, education, employment, housing, federal benefits, law enforcement, immigration, child welfare, transportation, critical infrastructure, and safety and environmental controls.
- Provide recommendations for managing risk in federal procurement of AI.

Additional notes from the OMB memo

The AI inventory that agencies must share publicly includes details on using safety-impacting and rights-impacting AI, which must follow minimum practices listed in the memo. Agencies must review each use of AI they are developing or using to determine whether it matches the definition of safety-impacting or rights-impacting.

Many healthcare AI use cases will be covered and governed under this memo. Among rights-impacting, AI-listed activities include decisions regarding medical devices, medical diagnostic tools, clinical diagnosis and determination of treatment, medical or insurance health-risk assessments, drug-addiction risk assessments and associated access systems, suicide or other violence risk assessment, mental-health status detection or prevention, systems that flag patients for interventions, public insurance care-allocation systems, or health-insurance cost and underwriting processes.

The minimum practices include performing an impact assessment, including the intended purpose for AI and its expected benefit, potential risks of using AI, and the quality and appropriateness of the relevant data. Other practices include an independent evaluation of the relevant AI documentation to ensure that the system works appropriately, as intended, and that its expected benefits outweigh its potential risks. This documentation includes the impact assessment and results from testing AI performance in a real-world context. The independent reviewing authority must not have been directly involved in the system's development. Additionally, as a precautionary safeguard, agencies are encouraged to leverage pilots and limited releases, with strong monitoring, evaluation, and safeguards in place, to carry out the final stages of testing before a wider release.

Additional practices include conducting ongoing monitoring, establishing thresholds for periodic human review, and ensuring there is sufficient training, assessment, and oversight for AI operators to interpret and act on the AI's output. Also, agencies must notify negatively affected individuals when AI meaningfully influences the outcome of decisions specifically concerning them and develop appropriate remedy processes. Additionally, agencies should maintain a mechanism to opt out of AI functionality in favor of a human alternative where practicable and consistent with applicable law when affected people reasonably expect an alternative or create unwarranted harmful impacts.

Conclusion

It will take time to unpack the full implications of the EO and OMB memo; however, it is clear the federal government will take greater actions to ensure a more ethical and responsible AI development and deployment landscape in the future. Additionally, there are terms shared in this new guidance that can be open to much interpretation and subjectivity. Future lobbying and arguments on what qualifies under the purview of compliance requirements may ensue. Eventually, certain obligations from federal agencies will likely ultimately flow down to federal contractors and companies that engage with the government, including accepting government funds.

There are many similarities between the guidance in the EO and OMB memo and an overall compliance program, such as designating chief AI officers, creating AI committees, reporting structures, risk management, training, policies, monitoring, and overall development of an AI program and strategy. Additionally, some of the specific processes listed in the guidance follow similar practices that are already in place in terms of compliance, risk management, privacy, and medical device practices. That means compliance professionals should be well adept at managing and coordinating such changes in the next frontier of regulatory change, which involves AI.

Previously, voluntary organizations and private industry led the push for ethical and responsible AI, including developing AI principles and high-level guardrails. Now, the U.S. government is providing a blueprint for its future expectations and will continue to push the industry to adapt to the ever-changing AI landscape, which will inevitably include regulations governing AI usage.

Takeaways

- The United States—which has relatively been lagging in substantive artificial intelligence (AI) legislation—has issued an Executive order (EO) that now puts AI governance and risk management in full scope at the federal government level.
- The EO on AI informs the safe, secure, and trustworthy development and use of AI focuses on AI safety and security, privacy, equity and civil rights, consumers and workers issues, promoting innovation and competition, and advancing American technology leadership around the world.
- The subsequent Office of Management and Budget draft memo focuses on three main areas: (1) strengthening AI governance, (2) advancing responsible AI innovation, and (3) managing risks from using AI.
- Many of these federal AI standards are similar to standards in compliance today.
- As such, compliance professionals should be well adept at managing and coordinating such changes in the next frontier of AI regulatory change.

[1] European Parliament, “Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI,” news release, September 20, 2023, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

[2] International Association of Privacy Professionals, “Global AI Legislation Tracker,” September 2023, https://iapp.org/resources/article/global-ai-legislation-tracker/.

[3] National Security Commission on Artificial Intelligence, *Final Report: National Security Commission on Artificial Intelligence*, accessed January 3, 2024, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[4] Latham & Watkins, “China’s New AI Regulations,” Client Alert, no. 3110, August 16, 2023, https://www.lw.com/en/admin/upload/SiteAttachments/Chinas-New-AI-Regulations.pdf.

[5] The White House, “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” October 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[6] Shalanda D. Young, “Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence,” memo, Office of Management and Budget, accessed January 3, 2024, https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf.