COSMOS
Navigate the Compliance Universe

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.