Biden to Issue First Regulations on Artificial Intelligence Systems

In an order to be issued on Monday, the White House will outline requirements that the most advanced A.I. products be tested to assure they cannot be used to produce weapons, among other regulations.

By David E. Sanger and Cecilia Kang
New York Times

President Biden will issue an executive order on Monday outlining the federal government's first regulations on artificial intelligence systems. They include requirements that the most advanced A.I. products be tested to assure that they cannot be used to produce biological or nuclear weapons, with the findings from those tests reported to the federal government.

The testing requirements are a small but central part of what Mr. Biden, in a speech scheduled for Monday afternoon, is expected to describe as the most sweeping government action to protect Americans from the potential risks brought by the huge leaps in A.I. over the past several years.

The regulations will include recommendations, but not requirements, that photos, videos and audio developed by such systems be watermarked to make clear that they were created by A.I. That reflects a rising fear that A.I. will make it far easier to create "deep fakes" and convincing disinformation, especially as the 2024 presidential campaign accelerates.

The United States recently restricted the export of high-performing chips to China to slow its ability to produce so-called large language models, the massing of data that has made programs like ChatGPT so effective at answering questions and speeding tasks. Similarly, the new regulations will require companies that run cloud services to tell the government about their foreign customers.

Mr. Biden's order will be issued days before a gathering of world leaders on A.I. safety organized by Britain's prime minister, Rishi Sunak. On the issue of A.I. regulation, the United States has trailed the European Union, which has been drafting new laws, and other nations, like China and Israel, that have issued proposals for regulations. Ever since ChatGPT, the A.I.-powered chatbot, exploded in popularity last year, lawmakers and global regulators have grappled with how artificial intelligence might alter jobs, spread disinformation and potentially develop its own kind of intelligence.

"President Biden is rolling out the strongest set of actions any government in the world has ever taken on A.I. safety, security and trust," said Bruce Reed, the White House

deputy chief of staff. “It’s the next step in an aggressive strategy to do everything on all fronts to harness the benefits of A.I. and mitigate the risks.”

The new U.S. rules, some of which are set to go into effect in the next 90 days, are likely to face many challenges, some legal and some political. But the order is aimed at the most advanced future systems, and it largely does not address the immediate threats of existing chatbots that could be used to spread disinformation related to Ukraine, Gaza or the presidential campaign.

The administration did not release the language of the executive order on Sunday, but officials said that some of the steps in the order would require approval by independent agencies, like the Federal Trade Commission.

The order affects only American companies, but because software development happens around the world, the United States will face diplomatic challenges enforcing the regulations, which is why the administration is attempting to encourage allies and adversaries alike to develop similar rules. Vice President Kamala Harris is representing the United States at the conference in London on the topic this week.

The regulations are also intended to influence the technology sector by setting first-time standards for safety, security and consumer protections. By using the power of its purse strings, the White House’s directives to federal agencies aim to force companies to comply with standards set by their government customers.

“This is an important first step and, importantly, executive orders set norms,” said Lauren Kahn, a senior research analyst at the Center for Security and Emerging Technology at Georgetown University.

The order instructs the Department of Health and Human Services and other agencies to create clear safety standards for the use of A.I. and to streamline systems to make it easier to purchase A.I. tools. It orders the Department of Labor and the National Economic Council to study A.I.’s effect on the labor market and to come up with potential regulations. And it calls for agencies to provide clear guidance to landlords, government contractors and federal benefits programs to prevent discrimination from algorithms used in A.I. tools.

But the White House is limited in its authority, and some of the directives are not enforceable. For instance, the order calls for agencies to strengthen internal guidelines to protect personal consumer data, but the White House also acknowledged the need for privacy legislation to fully ensure data protection.

To encourage innovation and bolster competition, the White House will request that the F.T.C. step up its role as the watchdog on consumer protection and antitrust violations. But the White House does not have authority to direct the F.T.C., an independent agency, to create regulations.

Lina Khan, the chair of the trade commission, has already signaled her intent to act more aggressively as an A.I. watchdog. In July, the commission opened an investigation into OpenAI, the maker of ChatGPT, over possible consumer privacy violations and accusations of spreading false information about individuals.

“Although these tools are novel, they are not exempt from existing rules, and the F.T.C. will vigorously enforce the laws we are charged with administering, even in this new market,” Ms. Khan wrote in a guest essay in The New York Times in May.

The tech industry has said it supports regulations, though the companies disagree on the level of government oversight. Microsoft, OpenAI, Google and Meta are among 15 companies that have agreed to voluntary safety and security commitments, including having third parties stress-test their systems for vulnerabilities.

Mr. Biden has called for regulations that support the opportunities of A.I. to help in medical and climate research, while also creating guardrails to protect against abuses. He has stressed the need to balance regulations with support for U.S. companies in a global race for A.I. leadership. And toward that end, the order directs agencies to streamline the visa process for highly skilled immigrants and nonimmigrants with expertise in A.I. to study and work in the United States.

The central regulations to protect national security will be outlined in a separate document, called the National Security Memorandum, to be produced by next summer. Some of those regulations will be public, but many are expected to remain classified — particularly those concerning steps to prevent foreign nations, or nonstate actors, from exploiting A.I. systems.

A senior Energy Department official said last week that the National Nuclear Security Administration had already begun exploring how these systems could speed nuclear proliferation, by solving complex issues in building a nuclear weapon. And many officials have focused on how these systems could enable a terror group to assemble what is needed to produce biological weapons.

Still, lawmakers and White House officials have cautioned against moving too quickly to write laws for A.I. technologies that are swiftly changing. The E.U. did not consider large language models in its first legislative drafts.

“If you move too quickly in this, you may screw it up,” Senator Chuck Schumer, Democrat of New York and the majority leader, said last week.