Government Overreach in the Presidential Executive Order on Artificial Intelligence

March 21, 2024

Testimony Before the House Subcommittee on Cybersecurity, Information Technology, and Government Innovation
Hearing: White House Overreach on AI

Neil Chilson, Head of AI Policy, The Abundance Institute[1]

Thank you, Chairwoman Mace, Ranking Member Connolly, and subcommittee members for having me today to talk about the Biden Executive Order on Artificial Intelligence. I am Neil Chilson, the Head of AI Policy at the Abundance Institute, a former Chief Technologist at the Federal Trade Commission (FTC), and a past advisor to acting FTC Chair Maureen K. Ohlhausen.

The Abundance Institute is a mission-driven nonprofit dedicated to creating an environment for emerging technologies to germinate, develop, and thrive in order to perpetually expand widespread human prosperity and abundance.

Now is a crucial time for this mission, as the many technologies of artificial intelligence launch us toward greater prosperity and abundance. Intelligence is our most vital resource. It is the tool with which humanity has overcome countless challenges. Every breakthrough technology, scientific discovery, business success, art piece, and literary work stems from human intellect. Often, turning intellect into material progress involves massive collaboration and coordination, generating intelligent outcomes beyond any one person's capabilities. Tools amplifying human intelligence, therefore, have vast potential. AI promises to help humanity create a healthier, safer, more productive, more artistic, more interesting, and more enjoyable world.

However, to develop and deploy AI to its fullest potential, we need the right cultural and regulatory environment. The Biden Administration's recent "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" does not cultivate that

[1] The views expressed in this testimony are those of the author and do not necessarily reflect the views of the Abundance Institute.

environment; indeed, its likely effect is to add regulatory burdens to AI and to software development generally. Most importantly, the EO imposes these new burdens without Congressional authorization.

Background on the Unprecedented AI Executive Order

On October 30, 2023, President Biden issued an "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."[2] The EO is a dense roadmap for government intervention over the next several years, complete with dozens of deadlines, reports, and policy deliverables. Its length and specificity make its regulatory impact unprecedented.

The AI Executive Order is unusual in form. It is atypically long, just shy of 20,000 words. Of the over nine thousand Presidential executive orders identified and collected by the American Presidency Project at University of California-Santa Barbara, the AI EO is the third longest Executive Order in American history.[3] The only EOs that are longer are a 1951 President Truman EO setting forth the entire manual for military Court Martial Procedures, and President Carter's 1980 update to that manual.[4] Most executive orders are much shorter than the AI EO, which is 88 times longer than the median executive order. Indeed, many of the most important executive orders are less than a dozen pages long.[5]

The EO is also unusual in substance. News coverage has focused on the EO's obligations for companies that develop large foundational models and the companies that supply the computational resources to develop such models. These obligations deserve attention, especially from Congressional oversight committees like this one, because, as I will discuss later, the EO imposes that new regulation without any Congressional authorization. Also worth discussing, however, is the EO directives to dozens of agencies and federal officials to engage in a wide range of activities to govern AI. By my count these activities include 136 different deliverables such as: seventeen reports, thirty-two new guidance documents, eleven proposed regulations, and dozens of new projects, processes, plans, and events.

---

[2] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (Oct. 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/.

[3] The American Presidency Project, "Executive Orders," https://www.presidency.ucsb.edu/statistics/data/executive-orders. *See also* March 11, 2024 e-mail and attachment from John Woolley and Gerhard Peters, co-directors of the American Presidency Project, on file with the author.

[4] *See*, Executive Order 10214, "Prescribing the Manual for Courts-Martial, United States" (Feb. 8, 1951), https://www.presidency.ucsb.edu/documents/executive-order-10214-prescribing-the-manual-for-courts-martial-united-states-1951 *and* Executive Order 12198, "Prescribing Amendments to the Manual for Courts-Martial, United States, 1969 (Revised Edition)" (Mar. 12, 1980), https://www.presidency.ucsb.edu/documents/executive-order-12198-prescribing-amendments-the-manual-for-courts-martial-united-states.

[5] *See, e.g.*, Executive Order 12866 "Regulatory Planning and Review," issued by President Clinton on September 30, 1993, (establishes the process by which the Office of Information and Regulatory Affairs reviews all federal regulation), https://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf.

Executive orders have had many different functions historically, but it is rare for a single EO to issue dozens of specific new policy directives to dozens of agencies and official.[6] Reshaping the entire federal government's role on a single domestic policy topic is traditionally and constitutionally Congress's job.

Not all of the AI EO-directed actions are unauthorized. Many of the directed actions are information gathering efforts or exhortations to apply existing regulatory authority as necessary and relevant to this new technology. While one might question whether such efforts are worth the costs or will produce useful results, the President has the authority to issue them. Some of these authorized actions are advisable. Indeed, the EO is on its strongest legal and policy grounds when it directs the Federal government to assess and manage its own use of this new technology.[7]

Had the EO focused on the government's own use of AI, it would have been on solid legal ground. However, the EO goes far beyond that safe territory.

Misuse of the Defense Production Act

EO Section 4.2 directs the Secretary of Commerce to impose new obligations on private companies. These obligations would require companies "developing or demonstrating an intent to develop potential dual-use foundation models" to provide the government with significant amounts of highly sensitive business and technical information.[8] The types of information that would seem to be required include, among other things:

- all ongoing or planned training of certain AI models;
- cybersecurity measures to protect training integrity and access to trained models;
- ownership and possession of certain AI models;
- the performance of certain AI models in government-established red-team testing regimes; and
- any mitigations to improve the performance of certain AI models on these government-established tests.

Section 4.2(a) also requires that companies that "acquire, develop, or purchase" computing clusters above a certain threshold must report the location and computing power of such clusters.

---

[6] Directing action in dozens of agencies in a single EO is not entirely unprecedented. Perhaps the closest precedent is President Nixon's Executive Order 11490, "Assigning Emergency Preparedness Functions to Federal Departments and Agencies," https://www.federalregister.gov/executive-order/11490. But that was a managerial EO that consolidated 21 pre-existing EOs and two pre-existing Defense Mobilization orders. *See* Executive Order 11490 § 101.

[7] *See, e.g.*, EO Section 7.1(b) (directing efforts with regard to the use of AI in the criminal justice system).

[8] EO Section 4.2(a)(i).

As a letter from twenty State Attorneys General to NTIA summarizes it, Section 4.2 of the EO requires such companies "to report to the federal government on their 'ongoing or planned activities,' to conduct various tests based on federal regulations, and to report to the government on the results of those tests."[9]

The EO imposes these new obligations in pursuit of "the continuous availability of safe, reliable, and effective AI in accordance with the Defense Production Act."[10] This generic reference to the Defense Production Act (DPA) is the only statutory authority cited for the regulations imposed in Section 4.2(a). But the Defense Production Act cannot support these new obligations, for at least three reasons.

First, the Defense Production Act empowers the President in emergencies to spur defense-related production. It does not permit the President to micromanage industries on an "ongoing" basis.[11] The DPA is a Korean War-era law intended to ensure the government has access to materials and services necessary to defend the country. It is typically used to put government contracts at the front of the manufacturing line (Title I), and sometimes to spend money to expand productive capacity in defense-essential capabilities (Title III).[12] Here, though, the Biden administration is not using the DPA to spur the production of AI or computing facilities for government use and to support national security. Instead, the EO deploys the DPA to demand highly confidential documents from companies that may not even have a contractual relationship with the government and to drive the adoption of government-established quality control measures for commercially available products to be used by normal Americans and businesses.

The EO does not identify which specific DPA provision authorizes EO Section 4.2. It would appear that Section 705 of the DPA is the most relevant.[13] However, that section is most commonly used for "industrial base assessments" to inform where Title III authorities need to be used to expand productive capacity.[14] Yet Section 4.2 does not expand AI production capacity; if anything, it discourages production by imposing new requirements on foundational models above a specific capacity.[15]

The primary products being "produced" by this use of the Defense Production Act will be reams of filings to the Federal Government and a legal precedent for unilateral Presidential regulation of the economy.

---

[9] Letter from Utah Attorney General Sean Reyes *et al.* to Secretary of Commerce Gina Raimondo, Feb.2, 2024, https://attorneygeneral.utah.gov/wp-content/uploads/2024/02/2024-02-02_Comment_response_letter_on_NIST_RFI_re_AI.pdf.

[10] EO Section 4.2(a).

[11] EO Section 4.2(a)(i).

[12] *See* Congressional Research Service, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," at 8-9 and 13-14 (updated October 6, 2023), https://crsreports.congress.gov/product/pdf/R/R43767 (hereafter, "CRS DPA Report").

[13] 50 U.S. Code §4555(a).

[14] CRS DPA Report at 15.

[15] EO Section 4.2(b).

Second, the DPA is not a shortcut around the U.S. Constitution. The Constitution assigns the power to make the laws to Congress, not to the Executive branch.[16] Indeed, Congress is actively considering a swath of artificial intelligence-related bills.[17] If Congress chooses to act deliberately on a specific issue, the President cannot therefore usurp that decision by stepping in and regulating, with merely a general reference to the DPA.

Third, the DPA is an emergency power, but there is no emergency here. Current AI developments are rapid, but they build on a long trend in machine learning that dates back at least to the development of neural networks algorithms in the 1970s.[18] The transformer architecture that underlies many increasingly popular generative AI tools, such as ChatGPT, was released by Google researchers in August 2017.[19]

The EO claims that "[t]he rapid speed at which AI capabilities are advancing compels the United States to lead in this moment for the sake of our security, economy, and society."[20] But continued rapid AI development poses no emergency threat to U.S. leadership because the U.S. already has a significant lead in the development of AI and AI companies.[21]

The EO offers no indication of what emergency it seeks to address or when it will end. Indeed, Section 4.2 imposes "ongoing" obligations, suggesting the Administration sees no end to the alleged emergency.

The EO does list potential societal harms, worrying that AI misuse could "exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; [and] stifle competition."[22] Section 2 elaborates on many of these potential harms. But even with elaboration none of these look like the kinds of emergencies the DPA is intended to address. Most are traditional consumer protection, civil rights, labor, and competition issues where Congress has proven willing and able to create legislation.[23] While such issues are important, they are not national security emergencies that justify upending our democratic tradition of legislative lawmaking.

Section 1 does mention that AI could "pose risks to national security." Section 2 fleshes out these concerns: "Artificial Intelligence must be safe and secure," says the EO, which "requires

---

[16] U.S. Const. art. I § 1 ("All legislative Powers herein granted shall be vested in a Congress of the United States….")
[17] The American Action Forum's AI Legislation Tracker shows 78 active AI-related bills in Congress. *See* https://www.americanactionforum.org/list-of-proposed-ai-bills-table/.
[18] *See* F. Rosenblatt (1958), The Perceptron: A Probabilistic Model For Information Storage And Organization In The Brain, Psychological Review. 65 (6): 386–408, https://doi.org/10.1037/h0042519.
[19] Ashish Vaswani *et al.*, Attention is All You Need, https://doi.org/10.48550/arXiv.1706.03762.
[20] EO Section 1.
[21] Tortoise Media, The Global AI Index (last visited Mar. 18, 2024) https://www.tortoisemedia.com/intelligence/global-ai/ (scoring the U.S. at the top of three main pillars: implementation, innovation, and investment).
[22] EO Section 1.
[23] "Disinformation" is an area where the First Amendment limits intervention from any branch of government.

addressing AI systems' most pressing security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers."[24]

However, if Section 4.2 is intended to reduce those risks to national security, its use of the DPA still overreaches. The DPA is intended to reduce one very specific type of risk to national security: threats to "the ability of the domestic industrial base to supply materials and services" needed for national defense and disaster recovery.[25] The EO does not mention such risk. Even had it done so, there is no emergency shortfall in the ability of the domestic industrial base to supply AI capabilities; indeed, "AI capabilities are advancing" at a "rapid speed."[26]

In sum, Section 4.2 of the EO imposes new regulations on private companies that are not and cannot be justified by a general reference to the Defense Production Act.

Expansive Definition of AI and the Effect on the Software Industry

Outside of the improper use of the DPA to impose direct regulation on some AI and hardware companies, the EO's broad definition of AI and its many directives to Federal agencies threaten to refactor software development in the United States.

Despite the fact that there is no expert consensus on the definition of AI,[27] the EO sets forth the following definition AI:

> The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.[28]

This broad definition includes far more software than the large language models or "generative AI" tools that have generated massive attention since the launch of ChatGPT. Indeed, as former Microsoft executive Steven Sinofsky has pointed out, the EO's AI definition likely covers 1980's era financial software.[29] It also appears to cover algorithms used for: social media content

[24] EO Section 2.
[25] 50 U.S.C. § 4502(a)(1).
[26] EO Section 1.
[27] Neil Chilson, Testimony Before the United States Senate Committee on Rules and Administration, Hearing: AI and the Future of our Elections at 2 (Sept. 27 2023), https://www.rules.senate.gov/imo/media/doc/chilson_testimony.pdf.
[28] EO Section 3(b).
[29] Steven Sinofsky, "211. Regulating AI by Executive Order is the Real AI Risk" (Nov. 1, 2023), https://hardcoresoftware.learningbyshipping.com/p/211-regulating-ai-by-executive-order.

moderation and feeds; targeted advertising; search engine algorithms; in-game bots; insurance models; any number of financial tools; and more. In short, the EO defines AI to include a wide swath of software.

The EO borrows this definition from the National AI Initiative Act of 2020, a bill intended to boost government agency spending on AI technology.[30] There, a vague and over-inclusive definition received little attention because it posed little risk: no legal consequences followed for software developers that entirely ignored the National AI Initiative Act.

Here, companies will not have the luxury of ignorance. Dozens of agencies will be using the EO's expansive definition to develop new guidance and regulations.

Future software developers could labor under several categories of obligations from the EO separate from the already-discussed mandates in Section 4.2. The EO's other provisions fall into three categories: 1) requirements on how agencies should act as purchasers and users of AI; 2) requests or suggestions that agencies apply their existing authorities to this new topic area; and 3) calls for agencies to issue guidance, best practices, standards, and other non-mandatory soft-law provisions.

Thus, portions of the EO will affect companies that sell software to the federal government or those that sell private sector software for use in critical infrastructure or a regulated industry, such as human resources, bioengineering, transportation, education, healthcare, housing, or energy.

For example, the EO directs the Secretary of Health and Human Services to establish quality assurance programs for software in the health and human services sector.[31] Specifically, HHS is to "determine whether AI-enabled technologies in the health and human services sector maintain appropriate levels of quality, including … enabling pre-market assessment and post-market oversight of AI-enabled healthcare-technology algorithmic system performance against real-world data."[32] The broad definition of AI in the Executive Order means every healthcare software provider ought to follow such developments and ensure their views are represented to HHS.

The EO also seeks to impose new obligations on software *users*. For example, the EO charges the Secretary of Labor with "[d]evelop[ing] and publish[ing] principles and best practices for employers that could be used to mitigate AI's potential harms to employees' well-being and maximize its potential benefits."[33] Given the broad definition of AI, this proceeding could impact every U.S. employer.

[30] 15 U.S.C. § 9411.
[31] EO Section 8(b)(ii).
[32] EO Section 8(b)(ii).
[33] EO Section 6(b)(i).

Certain initiatives in the EO will apply across the economy. For example, the EO "encourages" the Federal Trade Commission (FTC) to "consider [using] its rulemaking authority …. to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI."[34] The FTC is nominally an independent agency overseen by Congress, which is why the EO "encourages" action rather than directing it. But the President nominated the commissioners and his encouragement will usually drive results.

Much of the agency response to the EO will be in the form of guidance documents. Industry may be tempted to ignore the development and deployment of such non-mandatory instruments. That would be a mistake, because such guidance documents will lay the groundwork for follow-on action by other parts of the federal government. For example, the FTC has often used guidance in its law enforcement actions. As the U.S.'s general consumer protection agency, the FTC is charged with redressing "unfair and deceptive acts and practices."[35] If a company claims to follow specific standards or guidelines but doesn't, the FTC may have a deception case. And the FTC has often relied on guidance and standards when establishing whether a particular business practice is unfair. For example, in data security cases, the FTC often points to established best practices to determine whether a company that has suffered a data breach was acting "unfairly." If the FTC determines that a company was not following best practices, that could lead to significant financial costs and mandatory FTC-enforced constraints on the business's operations.

There are other ways that the EO could have a real impact on the broader software industry. For example, the EO charges some agencies with proposing legislation. And the testing standards that NIST is charged with developing could also be adopted by courts as a standard of care in tort cases.

Meanwhile, the EO's application to open source software is unclear. The order's expansive definition of AI means that open source systems could struggle to comply with new regulations. In an open letter, many leading AI technologists, academics, and investors pushed back against the EO, describing it as a threat to open source software and systems as a competitive counterbalance to proprietary platforms.[36]

Such comprehensive regulation of the development and use of software would be a new approach for the US. There is no Federal Computer Agency responsible for regulating software. Instead, we address harms involving the use of software through a combination of broad-based laws governing fraud, civil rights, unfair practices, or unsafe products. Tort law such as negligence and product liability cases provide court-based remedies for other harms.

---

[34] EO Section 5.3(a).
[35] 15 U.S. Code § 45.
[36] Letter from Marc Andreessen, *et al*. to President Joseph R. Biden, Jr. (Nov. 2, 2023), https://x.com/martin_casado/status/1720517026538778657?s=20.

The existing diverse set of approaches is appropriate, because software is so broad in application that no single agency has the necessary specialized knowledge to govern every application of the technology. As a result, rather than regulating software generally, the U.S. regulates certain industries, most of which happen to use software, such as medical devices and aviation. And where academics, researchers, and practitioners need to coordinate on technical issues, they have used non-governmental standard-setting organizations like the ACM and IEEE to define, for example, "floating point operations."[37]

Motivated by concerns over generative artificial intelligence, the EO directs a new regime of regulatory oversight for the software industry overall. The dozens of guidance and best practices documents spurred by the EO will have legal consequences for the software development industry and even for software users.

Even if it were desirable to revise the U.S. approach to software regulation, using a Presidential Executive Order to render such a dramatic change to the regulatory landscape is inappropriate. Such a potential sea change in one of America's most vibrant industries deserves to be considered, refined, and decided by Congress.

Conclusion

The Executive Order is largely a missed opportunity to set forth a positive vision for the future of AI use while shoring up civil liberties from government misuse of these technologies. But not only does the EO strike the wrong policy balance – it also usurps Congress, abusing the DPA to impose new regulations and spurring a deluge of regulatory action that will affect the entire software industry. This overreach calls for continued congressional oversight, democratic accountability, and potentially legislative or judicial course correction.

Thank you, and I look forward to your questions.

[37] Interestingly, the EO defines a "floating-point operation" but rather than rely on industry standards such as IEEE 754-2019, the EO definition appears to have been taken from Wikipedia. *Compare* EO Section 3(m) ("represented on computers by *an integer of fixed precision scaled by an integer exponent of a fixed base*")(emphasis added) *with* Floating-point Arithmetic, Wikipedia, https://en.wikipedia.org/wiki/Floating-point_arithmetic (last visited Mar. 18, 2023)("using an integer with a fixed precision, called the significand, scaled by an integer exponent of a fixed base").