INSTITUTE
FOR LAW & AI

Existing authorities for oversight of frontier AI models

LawAI Working Paper Working Paper Series, No. 1-2024
Charlie Bullock, Suzanne Van Arsdale, Mackenzie Arnold, Matthijs Maas, and Christoph Winter

July 2024

law-ai.org

Existing authorities for oversight of frontier AI models

Institute for Law & AI

July 2024 | Charlie Bullock,[*] Suzanne Van Arsdale,[†] Mackenzie Arnold,[‡] Matthijs Maas,[**] and Christoph Winter[††]

Abstract

It has been suggested that a national frontier AI governance strategy should include a comprehensive regime for tracking and licensing the creation and dissemination of frontier models and critical hardware components ("AI Oversight"). A robust Oversight regime would almost certainly require new legislation. In the absence of new legislation, however, it might be possible to accomplish some of the goals of an AI Oversight regime using existing legal authorities. This memorandum discusses a number of existing authorities in order of their likely utility for AI Oversight. The existing authorities that appear to be particularly promising include the Defense Production Act, the Export Administration Regulations, the International Emergency Economic Powers Act, the use of federal funding conditions, and Federal Trade Commission consumer protection authorities. Somewhat less promising authorities discussed in the memo include § 606(c) of the Communications Act of 1934, Committee on Foreign Investment in the United States review, the Atomic Energy Act, copyright and antitrust laws, the Biological Weapons Anti-Terrorism Act, the Chemical Weapons Convention Implementation Act, and the Federal Select Agent Program.

Cite as: Charlie Bullock et al., *Existing authorities for oversight of frontier AI models*, Institute for Law & AI (July 2024), https://law-ai.org/existing-authorities-for-oversight.

[*] Corresponding author. Institute for Law & AI, Cambridge, MA, USA. Email: charlie.bullock@law-ai.org
[†] Institute for Law & AI, Cambridge, MA, USA. Email: suzanne.vanarsdale@law-ai.org
[‡] Institute for Law & AI, Cambridge, MA, USA. Email: mackenzie.arnold@law-ai.org
[**] Institute for Law & AI, Cambridge, MA, USA. / Leverhulme Centre for the Future of Intelligence, University of Cambridge, Cambridge, United Kingdom. ORCID iD: 0000-0002-6170-9393. Email: mmm71@cam.ac.uk
[††] Instituto Tecnológico Autónomo de México, Mexico City, Mexico / Harvard University, Cambridge, MA, USA / Institute for Law & AI, Cambridge, MA, USA. Email: christoph_winter@fas.harvard.edu.

It has been suggested that frontier artificial intelligence ("AI") models may in the near future pose serious risks to the national security of the United States—for example, by allowing terrorist groups or hostile foreign state actors to acquire chemical, biological, or nuclear weapons, spread dangerously compelling personalized misinformation on a grand scale, or execute devastating cyberattacks on critical infrastructure. Wise regulation of frontier models is, therefore, a national security imperative, and has been recognized as such by leading figures in academia,[1] industry,[2] and government.[3]

One promising strategy for governance of potentially dangerous frontier models is "AI Oversight." AI Oversight is defined as a comprehensive regulatory regime allowing the U.S. government to:

1) Track and license hardware for making frontier AI systems ("AI Hardware")
2) Track and license the creation of frontier AI systems ("AI Creation"), and
3) License the dissemination of frontier AI systems ("AI Proliferation").

Implementation of a comprehensive AI Oversight regime will likely require substantial new legislation. Substantial new federal AI governance legislation, however, may be many months or even years away. In the immediate and near-term future, therefore, government Oversight of AI Hardware, Creation, and Proliferation will have to rely on existing legal authorities. Of course, tremendously significant regulatory regimes, such as a comprehensive licensing program for a transformative new technology, are not typically—and, in the vast majority of cases, should not be—created by executive fiat without any congressional input. In other words, the short answer to the question of whether AI Oversight can be accomplished using existing authorities is "no." The remainder of this memorandum attempts to lay out the long answer.

Despite the fact that a complete and effective Oversight regime based solely on existing authorities is an unlikely prospect, a broad survey of the authorities that could in theory contribute to such a regime may prove informative to AI governance researchers, legal scholars, and policymakers. In the interests of casting a wide net and giving the most complete possible picture of all plausible or semi-plausible existing authorities for Oversight, the included authorities were intentionally selected with an eye towards erring on the side of overinclusiveness. Therefore, this memo includes some authorities which are unlikely to be used, authorities which would only indirectly or partially contribute to Oversight, and authorities which would likely face serious legal challenges if used in the manner proposed.

Each of the eleven sections below discusses one or more existing authorities that could be used for Oversight and evaluates the authority's likely relevance. The sections are listed in descending order of evaluated relevance, with the more important and realistic authorities coming first and the more speculative or tangentially relevant authorities bringing up the rear. Some of the authorities discussed are "shovel-ready" and could be put into action immediately, while others would require some agency action, up to and including the promulgation of new regulations (but not new legislation), before being used in the manner suggested.

Included at the beginning of each Section are two bullet points addressing the aspects of Oversight to which each authority might contribute and a rough estimation of the authority's likelihood of use for Oversight. No

[1] See, e.g., Usman Anwar et al., *Foundational Challenges in Assuring Alignment and Safety of Large Language Models*, arXiv:2404.09932 (April 15, 2024).
[2] See, e.g., Anthropic, *Frontier Threats Red Teaming for AI Safety* (July 26, 2023); OpenAI, *Building an early warning system for LLM-aided biological threat creation* (January 31, 2024); Mary Phuong et al., *Evaluating Frontier Models for Dangerous Capabilities*, arXiv:2403.13793 (March 20, 2024).
[3] See, e.g., Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," § 4.2, 88 Federal Register 75191, October 30, 2023.

estimation of the likelihood that a given authority's use could be successfully legally challenged is provided, because the outcome of a hypothetical lawsuit would depend too heavily on the details of the authority's implementation for such an estimate to be useful.[4] The likelihood of use is communicated in terms of rough estimations of likelihood ("reasonably likely," "unlikely," etc.) rather than, e.g., percentages, in order to avoid giving a false impression of confidence, given that predicting whether a given authority will be used even in the relatively short term is quite difficult.

The table below contains a brief description of each of the authorities discussed along with the aspects of Oversight to which they may prove relevant and the likelihood of their use for Oversight.

Authority	Description	Potentially Relevant to:	Likelihood of use for Oversight:
Defense Production Act (DPA) Title VII	Authorizes broad range of information collecting activities, including industry surveys; authorizes President to sanction voluntary agreements between private interest, creating antitrust safe harbor; recruitment tools for govt talent	Tracking and Licensing Hardware & Creation; Licensing Proliferation	Already in use; reasonably likely to be used further
DPA Title I	Empowers President/agencies to prioritize certain contracts and to allocate resources to promote national defense	Licensing Hardware, Creation, & Proliferation	Reasonably likely
DPA Title III	Authorizes economic incentives (subsidies etc.) to promote national defense	Tracking and Licensing Hardware & Creation; Licensing Proliferation	Reasonably likely
Export Administration Regulations	Imposes licensing requirement on some exports, including software and data as well as tangible goods	Tracking and Licensing Hardware & Creation; Licensing Proliferation	Already in use; likely to be used further
Emergency Powers: International Emergency Economic Powers Act	Authorizes broad economic sanctions on individuals and entities during economic emergency	Tracking and Licensing Hardware & Creation; Licensing Proliferation	Already in use; may be used further
Emergency Powers: Communications Act of 1934 § 606(c)	Authorizes seizure or shutdown of electronic "devices," possibly including computers, servers, etc., in national emergency	Licensing Creation & Proliferation	Unlikely to be used
Federal Funding Conditions	Impose conditions on federal contracts (& perhaps on federal grants as well), requiring compliance with certain rules as condition of funding	Tracking and Licensing Hardware & Creation; Licensing Proliferation	Reasonably likely

[4] Readers who are interested in a more detailed discussion of the merits of legal challenges to specific implementation scenarios should feel free to reach out to the authors by email.

FTC Consumer Protection Authorities	Prohibits "unfair and deceptive practices" relating to commerce; authorizes conduct of industry studies	Tracking and Licensing Creation; Licensing Proliferation	Unlikely to be used for licensing; may be used for tracking
Committee on Foreign Investment in the United States	Reviews certain foreign investments in U.S. businesses and real estate; can recommend cancellation or unwinding of transactions	Tracking and Licensing Hardware & Creation	Unlikely to be used for Oversight directly; could facilitate
Atomic Energy Act	Prohibits disclosure of "Restricted Data" relating to nuclear weapons	Licensing Creation & Proliferation	Somewhat unlikely in the absence of new legislation
Copyright Law	May prohibit and penalize current state of the art approach to training Large Language Models	Licensing AI Creation & Proliferation	Unlikely to be used for Oversight directly; could facilitate
Antitrust Authorities	Prohibit anticompetitive conduct that harms consumers (could be used to create safe harbor for industry collaboration on safety research)	Tracking and Licensing Hardware & Creation	Unlikely to be used for Oversight directly; could facilitate
Biological Weapons Anti-Terrorism Act	Prohibits knowingly attempting development, production, or possession of biological agents for use as weapons	Licensing Creation & Proliferation	Unlikely
Chemical Weapons Convention Implementation Act	Prohibits knowingly assisting in the development, production, or possession of chemical weapons	Licensing Creation & Proliferation	Unlikely
Federal Select Agent Program	Authorizes establishment & support of safeguards & security measures to prevent access to certain biological agents and toxins	Tracking and Licensing Creation & Proliferation	Unlikely

Defense Production Act

→ Potentially applicable to: Licensing AI Hardware, Creation, and Proliferation; Tracking AI Hardware and Creation.
→ Already being used to track AI Creation; reasonably likely to be used again in the future in some additional AI Oversight capacity.

The Defense Production Act ("DPA")[5] authorizes the President to take a broad range of actions to influence domestic industry in the interests of the "national defense."[6] The DPA was first enacted during the Korean War and was initially used solely for purposes directly related to defense industry production. The DPA has since been reenacted a number of times—most recently in 2019, for a six-year period expiring in September 2025—and the statutory definition of "national defense" has been repeatedly expanded by Congress.[7] Today DPA authorities can be used to address and prepare for a variety of national emergencies.[8] The DPA was originally enacted with seven Titles, four of which have since been allowed to lapse. The remaining Titles—I, III, and VII—furnish the executive branch with a number of authorities which could be used to regulate AI hardware, creation, and proliferation.

Invocation of the DPA's information-gathering authority in Executive Order 14110

Executive Order 14110 relies on the DPA in § 4.2, "Ensuring Safe and Reliable AI."[9] Section 4.2 orders the Department of Commerce to require companies "developing or demonstrating an intent to develop dual-use foundation models" to "provide the Federal Government, on an ongoing basis, with information, reports, or records" regarding (a) development and training of dual-use foundation models and security measures taken to ensure the integrity of any such training; (b) ownership and possession of the model weights of any dual-use foundation models and security measures taken to protect said weights; and (c) the results of any dual-use foundation model's performance in red-teaming exercises.[10] The text of the EO does not specify which

[5] 50 U.S.C. §§ 4501 *et seq.*
[6] See 50 U.S.C. § 4502.
[7] The current statutory definition includes: "programs for military and energy production or construction, military or critical infrastructure assistance to any foreign nation, homeland security, stockpiling, space, and any directly related activity. Such term includes emergency preparedness activities conducted pursuant to title VI of The Robert T. Stafford Disaster Relief and Emergency Assistance Act [42 U.S.C. §§5195 et seq.] and critical infrastructure protection and restoration." 50 U.S.C. §4552(14).
[8] U.S. Congressional Research Service, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," p. 1 (R43767; October 6, 2023) ("[DPA] authorities may also be used to enhance and support domestic preparedness, response, and recovery from natural hazards, terrorist attacks, and other national emergencies."). In this century, the DPA has been used to, e.g., respond to the COVID-19 pandemic by ordering companies to produce facemasks and ventilators (Department of Homeland Security, The Defense Production Act Committee Report to Congress, Calendar Year 2020, September 20, 2021, p. 14); supply California with national gas to prevent blackouts during the 2000-2001 electricity crisis ("Causes and Lessons of the California Electricity Crisis," p. 30. Congressional Budget Office, September 2001); and block corporate mergers and acquisitions that would give Chinese companies ownership interests in U.S. semiconductor companies (Michael Brown and Pavneet Singh, "How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," p. 3 (Defense Innovation Unit Experimental 2018)).
[9] Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," § 4.2, 88 Federal Register 75191, October 30, 2023.
[10] Ibid.

provision(s) of the DPA are being invoked, but based on the language of EO § 4.2[11] and on subsequent statements from the agency charged with implementing EO § 4.2[12] the principal relevant provision appears to be § 705, from Title VII of the DPA.[13] According to social media statements by official Department of Commerce accounts, Commerce began requiring companies to "report vital information to the Commerce Department — especially AI safety test results.," no later than January 29, 2024.[14] However, no further details about the reporting requirements have been made public and no proposed rules or notices relating to the reporting requirements have been issued publicly as of the writing of this memorandum.[15]

Section 705 grants the President broad authority to collect information in order to further national defense interests,[16] which authority has been delegated to the Department of Commerce pursuant to E.O. 13603.[17] Section 705 authorizes the President to obtain information "by regulation, subpoena, or otherwise," as the President deems necessary or appropriate to enforce or administer the Defense Production Act. In theory, this authority could be relied upon to justify a broad range of government efforts to track AI Hardware and Creation. Historically, § 705 has most often been used by the Department of Commerce's Bureau of Industry and Security ("BIS") to conduct "industrial base assessment" surveys of specific defense-relevant industries.[18] For instance, BIS recently prepared an "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry" which concluded in February 2022.[19] BIS last conducted an assessment of the U.S. artificial intelligence sector in 1994.[20]

Republican elected officials, libertarian commentators, and some tech industry lobbying groups have questioned the legality of EO 14110's use of the DPA and raised the possibility of a legal challenge.[21] As no such lawsuit has yet been filed, it is difficult to evaluate § 4.2's chances of surviving hypothetical future legal challenges. The arguments against its legality that have been publicly advanced—such as that the "Defense Production Act is about production… not restriction"[22] and that AI does not present a "national

[11] Section 705 is the DPA provision regarding the "Authority of [The] President to Obtain Information," and specifically authorizes the executive to require private companies to provide "information," "reports," and "records" to the government. 50 U.S.C. § 4555(a). Section 4.2 of the EO mirrors this language by referencing the provision of "information, reports, or records" to the federal government by AI labs.
[12] See Hoover Institution Discussion, January 26, 2024, at 35:40–38:00 (Secretary of Commerce Gina Raimondo stating that "We're using the Defense Production Act... to do a survey requiring companies to share with us every time they train a new large language model, and share with us the results—the safety data—so we can review it."). In the past, Section 705 has usually been used to conduct "industrial base assessments," which are "industry-specific surveys." "Industrial Base Assessments," Bureau of Industry and Security.
[13] 50 U.S.C. § 4555.
[14] See Secretary Gina Raimondo, Tweets from January 29, 2024; U.S. Commerce Dept., Tweet from January 29, 2024.
[15] See "Transparency of AI EO Implementation: An Assessment 90 Days In," Caroline Meinhardt et al., February 21, 2024 (stating that "independent reporting" along with the public statements from Commerce supports the conclusion that the DPA reporting requirements have gone into effect, despite the fact that almost no information about the nature of the requirements has been made public other than the information contained in the EO).
[16] 50 U.S.C. § 4555(a).
[17] Executive Order 13603, "National Defense Resource Preparedness," § 104(d), 77 Federal Register 16651, March 16, 2012.
[18] U.S. Congressional Research Service, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," pp. 15–16 (R43767; October 6, 2023).
[19] Department of Commerce, "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry," February 24, 2022.
[20] Department of Commerce, "Critical Technology Assessment of the U.S. Artificial Intelligence Sector," August 1994.
[21] See Mohar Chatterjee & Brendan Bordelon, "The campaign to take down the Biden AI executive order." Politico, January 26, 2024; "Comment by States of Utah, Alabama, Arkansas, Florida, Idaho, Iowa, Kansas, Louisiana, Mississippi, Missouri, Montana, Nebraska, North Dakota, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Virginia, and West Virginia on RFI Related to NIST's Assignments under Sections 4.1, 4.5 and 11 of the Executive Order Concerning Artificial Intelligence," Office of the Attorney General of Utah, February 2, 2024.
[22] Chatterjee & Bordelon (2024).

emergency"[23]—are legally dubious, in this author's opinion.[24] However, § 705 of the DPA has historically been used mostly to conduct "industrial base assessments," i.e., surveys to collect information about defense-relevant industries.[25] When the DPA was reauthorized in 1992, President George H.W. Bush remarked that using § 705 during peacetime to collect industrial base data from American companies would "intrude inappropriately into the lives of Americans who own and work in the Nation's businesses."[26] While that observation is not in any sense legally binding, it does tend to show that EO 14110's aggressive use of § 705 during peacetime is unusual by historical standards and presents potentially troubling issues relating to executive overreach. The fact that companies are apparently to be required to report on an indefinitely "ongoing basis"[27] is also unusual, as past industrial base surveys have been snapshots of an industry's condition at a particular time rather than semipermanent ongoing information-gathering institutions.

DPA Title VII: voluntary agreements and recruiting talent

Title VII includes a variety of provisions in addition to § 705, a few of which are potentially relevant to AI Oversight. Section 708 of the DPA authorizes the President to "consult with representatives of industry, business, financing, agriculture, labor, and other interests in order to provide for the making by such persons, with the approval of the President, of voluntary agreements and plans of action to help provide for the national defense."[28] Section 708 provides an affirmative defense against any civil or criminal antitrust suit for all actions taken in furtherance of a presidentially sanctioned voluntary agreement.[29] This authority could be used to further the kind of cooperation between labs on safety-related issues that has not happened to date because of labs' fear of antitrust enforcement.[30] Cooperation between private interests in the AI industry could facilitate, for example, information-sharing regarding potential dangerous capabilities, joint AI safety research ventures, voluntary agreements to abide by shared safety standards, and voluntary agreements to pause or set

[23] Ibid.
[24] Invoking § 705 of the DPA does not require a "national emergency." Rather, the President is authorized to gather information "as may be necessary or appropriate, in his discretion, to the enforcement or administration of [the DPA] and the regulations or orders issued thereunder." 50 U.S.C. § 4555(a). At most, this might require the gathered information to be relevant to the "national defense," as that term is defined in the DPA. It seems likely that § 705 satisfies these requirements, given the expansive scope of the statutory definition of "national defense" and the fact that a number of AI technology categories, including "Next-generation AI " and "Safe and/or secure AI" have been designated as "Critical and Emerging Technologies" (i.e. "advanced technologies that are potentially significant to U.S. national security") by the National Science and Technology Council and are being treated as critical to national security by the Department of Defense. See Critical and Emerging Technologies List Update, pp. 1, 4. Fast Track Action Subcommittee on Critical and Emerging Technologies, February 2022; Joseph Clark, "Pentagon Official Lays Out DOD Vision for AI." Department of Defense, February 21, 2024. The argument that the DPA is meant to promote production, and therefore cannot be used to impose safety regulations that restrict production, seems similarly unconvincing. Safety testing is every bit as much a part of a sophisticated manufacturing process as injection molding or CNC machining. It is difficult to imagine a court finding that the security vulnerabilities of a new and potentially dangerous technology are irrelevant for purposes of the Defense Production Act, the purpose of which is to promote "the security of the United States." 50 U.S.C. § 4501. The DPA has frequently been used in the past to assess the security vulnerabilities of new technologies; for instance, BIS conducted a "U.S. Air Force C-17 Aircraft Supply Chain Impact Assessment" under § 705 in 2018 which dedicates more than 10 pages to analyzing physical and cyber-security related expenditures relating to the manufacturing of the aircraft in question.
[25] See James Baker, "A DPA for the 21st Century: Securing America's AI National Security Innovation Base" (Center for Security and Emerging Technology, 2021), 20.
[26] George H.W. Bush, Statement on Signing the Defense Production Act Amendments of 1992 (October 28, 1992).
[27] EO 14110 at § 4.2(a).
[28] 50 U.S.C. §4558(c)(1).
[29] U.S. Congressional Research Service, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," p. 16 (R43767; October 6, 2023).
[30] See Jide Alaga & Jonas Schuett, "Coordinated Pausing," arXiv:2310.00374, pp. 9–10 (Centre for the Governance of AI, 2023) (discussing concerns that pausing agreements would violate antitrust law).

an agreed pace for increases in the size of training runs for frontier AI models.[31] This kind of cooperation could facilitate an effective voluntary pseudo-licensing regime in the absence of new legislation.

Sections 703 and 710 of the DPA could provide effective tools for recruiting talent for government AI roles. Under § 703, agency heads can hire individuals outside of the competitive civil service system and pay them enhanced salaries.[32] Under § 710, the head of any governmental department or agency can establish and train a National Defense Executive Reserve ("NDER") of individuals held in reserve "for employment in executive positions in Government during periods of national defense emergency."[33] Currently, there are no active NDER units, and the program has been considered something of a failure because of underfunding and mismanagement since the Cold War,[34] but the statutory authority to create NDER units still exists and could be utilized if top AI researchers and engineers were willing to volunteer for NDER roles. Both §§ 703 and 710 could indirectly facilitate tracking and licensing by allowing information-gathering agencies like BIS or agencies charged with administering a licensing regime to hire expert personnel more easily.

DPA Title I: priorities and allocations authorities

Title I of the DPA empowers the President to require private U.S. companies to prioritize certain contracts in order to "promote the national defense." Additionally, Title I purports to authorize the President to "allocate materials, services, and facilities" in any way he deems necessary or appropriate to promote the national defense.[35] These so-called "priorities" and "allocations" authorities have been delegated to six federal agencies pursuant to Executive Order 13603.[36] The use of these authorities is governed by a set of regulations known as the Defense Priorities and Allocations System ("DPAS"),[37] which is administered by BIS.[38] Under the DPAS, contracts can be assigned one of two priority ratings, "DO" or "DX."[39] All priority-rated contracts take precedence over all non-rated contracts, and DX contracts take priority over DO contracts.[40]

Because the DPA defines the phrase "national defense" expansively,[41] the text of Title I can be interpreted to authorize a broad range of executive actions relevant to AI governance. For example, it has been suggested that the priorities authority could be used to prioritize government access to cloud-compute resources in times of crisis[42] or to compel semiconductor companies to prioritize government contracts for chips over preexisting

[31] For further discussion of the creation of an antitrust safe harbor to facilitate cooperation among labs designing frontier models, see Section 9 below.
[32] 50 U.S.C. § 4553.
[33] 50 U.S.C. § 4560.
[34] Fischer et al., "AI Policy Levers," p. 40.
[35] 50 U.S.C. § 4511(a)(2).
[36] Executive Order 13603, "National Defense Resource Preparedness," § 201, 77 Federal Register 16651, March 16, 2012. Under E.O. 13603, the Department of Agriculture wields Title I authority with respect to food resources, the Department of Energy with respect to energy, the Department of Health and Human Services with respect to health resources, the Department of Transportation with respect to civil transportation, the Department of Defense with respect to water resources, and the Department of Commerce with respect to "all other materials, services, and facilities." Ibid.
[37] 15 C.F.R. § 700
[38] Department of Homeland Security, The Defense Production Act Committee Report to Congress, Calendar Year 2020, September 20, 2021, p. 8.
[39] 15 C.F.R. § 700.3(a).
[40] Ibid.
[41] "The term 'national defense' means programs for military and energy production or construction, military or critical infrastructure assistance to any foreign nation, homeland security, stockpiling, space, and any directly related activity." 50 U.S.C. § 4552.
[42] James Baker, "A DPA for the 21st Century: Securing America's AI National Security Innovation Base" (Center for Security and Emerging Technology, 2021), 7.

contracts with private buyers.[43] Title I could also, in theory, be used for AI Oversight directly. For instance, the government could in theory attempt to institute a limited and partial licensing regime for AI Hardware and Creation by either (a) allocating limited AI Hardware resources such as chips to companies that satisfy licensing requirements promulgated by BIS, or (b) ordering companies that do not satisfy such requirements to prioritize work other than development of potentially dangerous frontier models.[44]

The approach described would be an unprecedentedly aggressive use of Title I, and is unlikely to occur given the hesitancy of recent administrations to use the full scope of the presidential authorities Title I purports to convey. The allocations authority has not been used since the end of the Cold War,[45] perhaps in part because of uncertainty regarding its legitimate scope.[46] That said, guidance from the Defense Production Act Committee ("DPAC"), a body that "coordinate[s] and plan[s] for . . . the effective use of the priorities and allocations authorities",[47] indicates that the priorities and allocations authorities can be used to protect against, respond to, or recover from "acts of terrorism, cyberattacks, pandemics, and catastrophic disasters."[48] If the AI risk literature is to be believed, frontier AI models may soon be developed that pose risks related to all four of those categories.[49]

The use of the priorities authority during the COVID-19 pandemic tends to show that, even in recognized and fairly severe national emergencies, extremely aggressive uses of the priorities and allocations authorities are unlikely. FEMA and the Department of Health and Human Services ("HHS") used the priorities authority to require companies to produce N95 facemasks and ventilators on a government-mandated timeline,[50] and HHS and the Department of Defense ("DOD") also issued priority ratings to combat supply chain disruptions and expedite the acquisition of critical equipment and chemicals for vaccine development as part of Operation Warp Speed.[51] But the Biden administration did not invoke the allocations authority at any point, and the priorities authority was used for its traditional purpose—to stimulate, rather than to prevent or regulate, the industrial production of specified products.

---

[43] Sophie-Charlotte Fischer et al., "AI Policy Levers: A Review of the U.S. Government's Tools to Shape AI Research, Development, and Deployment," p. 20 (Centre for the Governance of AI, Future of Humanity Institute, University of Oxford, 2021).

[44] The DPAS currently allows businesses to choose not to accept priority-rated orders under certain limited circumstances, such as when the proposed contract is for a good that the company does not produce or a service the company does not provide. See 15 C.F.R. 700.13(c). However, this limitation is imposed by agency regulations rather than by the DPA itself, and does not limit the President's ability to "require acceptance and performance" of contracts pursuant to Title I via executive order. 50 U.S.C. § 4511; but see Baker, "A DPA for the 21st Century," at 17–18 (arguing that it is unclear whether, under Title I, businesses can legally be required to produce or provide goods or services that they do not ordinarily provide).

[45] Department of Homeland Security, The Defense Production Act Committee Report to Congress, Calendar Year 2019, September 17, 2020, p. 11.

[46] James Baker suggests that Presidents may have been hesitant to invoke the allocations authority because its facial overbroadness raises concerns about executive overreach. Baker, "A DPA for the 21st Century," at 22–23.

[47] 50 U.S.C. § 4567(a).

[48] Department of Homeland Security, The Defense Production Act Committee Report to Congress, Calendar Year 2020, September 20, 2021, p. 21.

[49] See, e.g., Dan Hendrycks *et al.*, "An Overview of Catastrophic AI Risks," arXiv:2306.12001 (2023).

[50] Department of Homeland Security, The Defense Production Act Committee Report to Congress, Calendar Year 2020, September 20, 2021, p. 14.

[51] GAO Report to Congressional Addresses, February 2021, Operation Warp Speed.

DPA Title III: subsidies for industry

Title III of the DPA authorizes the President to issue subsidies, purchase commitments and purchases, loan guarantees, and direct loans to incentivize the development of industrial capacity in support of the national defense.[52] Title III also establishes a Defense Production Act Fund, from which all Title III actions are funded and into which government proceeds from Title III activities and appropriations by Congress are deposited.[53] The use of Title III requires the President to make certain determinations, including that the resource or technology to be produced is essential to the national defense and that Title III is the most cost-effective and expedient means of ensuring the shortfall is addressed.[54] The responsibility for making these determinations is non-delegable.[55] The Title III award program is overseen by DOD.[56]

Like Title I, Title III authorities were invoked a number of times in order to address the COVID-19 pandemic. For example, DOD invoked Title III in April 2020 to award $133 million for the production of N-95 masks and again in May 2020 to award $138 million in support of vaccine supply chain development.[57] More recently, President Biden issued a Presidential Determination in March 2023 authorizing Title III expenditures to support domestic manufacturing of certain important microelectronics supply chain components—printed circuit boards and advanced packaging for semiconductor chips.[58]

It has been suggested that Title III subsidies and purchase commitments could be used to incentivize increased domestic production of important AI hardware components, or to guarantee the purchase of data useful for military or intelligence-related machine learning applications.[59] This would allow the federal government to exert some influence over the direction of the funded projects, although the significance of that influence would be limited by the amount of available funding in the DPA fund unless Congress authorized additional appropriations. With respect to Oversight, the government could attach conditions intended to facilitate tracking or licensing regimes to contracts entered into under Title III.[60]

Export controls

- → Potentially applicable to: Licensing AI Hardware, Creation, and Proliferation
- → Already being used to license exports of AI Hardware; new uses relating to Oversight likely in the near future

[52] 50 U.S.C. §§ 4531–4533. In practice, the loan guarantee and direct loan authorities are never used, but the purchase commitment/purchasing authorities and subsidy authorities are used regularly. Jillian Stern, "The COVID-19 Pandemic and the Defense Production Act: Government Misuse and Failures," 51 Pub. Cont. L.J. 323, 332 (2022).
[53] U.S. Congressional Research Service, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," p. 12 (R43767; October 6, 2023).
[54] 50 U.S.C. § 4533(a)(5).
[55] Ibid.
[56] Office of the Assistant Secretary of Defense, Industrial Base Policy, "Defense Production Act Title III Overview."
[57] Stern, "The COVID-19 Pandemic and the Defense Production Act," at 334.
[58] Press Release, Dep't of Defense, "Defense Production Act Title III Presidential Determination for Printed Circuit Boards and Advanced Packaging Production Capability" (March 27, 2023).
[59] See Baker, "A DPA for the 21st Century," at 6 (suggesting that Title III incentives could be used to incentivize the establishment of a domestic industry for extreme ultraviolet lithography scanners).
[60] DOD typically awards Title III funds in the form of technology investment agreements. GAO Report to Congressional Committees, "Defense Production Act - Opportunities Exist to Increase Transparency and Identify Future Actions to Mitigate Medical Supply Chain Issues," p. 6 (November 2020). Technology investment agreements usually involve significant government oversight of the funded project. See 32 C.F.R. § 37.220(a). For a more thorough discussion of the potential use of federal contract conditions to facilitate Oversight, see Section 6 below.

Export controls are legislative or regulatory tools used to restrict the export of goods, software, and knowledge, usually in order to further national security or foreign policy interests. Export controls can also sometimes be used to restrict the "reexport" of controlled items from one foreign country to another, or to prevent controlled items from being shown to or used by foreign persons inside the U.S.

Currently active U.S. export control authorities include: (1) the International Traffic in Arms Regulations ("ITAR"), which control the export of weapons and other articles and services with strictly military applications;[61] (2) multilateral agreements to which the United States is a state party, such as the Wassenaar Arrangement;[62] and (3) the Export Administration Regulations ("EAR"), which are administered by BIS and which primarily regulate "dual use" items, which have both military and civilian applications.[63] This section focuses on the EAR, the authority most relevant to Oversight.

Export Administration Regulations

The EAR incorporate the Commerce Control List ("CCL").[64] The CCL is a list, maintained by BIS, of more than 3,000 "items" which are prohibited from being exported, or prohibited from being exported to certain countries, without a license from BIS.[65] The EAR define "item" and "export" broadly—software, data, and tangible goods can all be "items," and "export" can include, for example, showing controlled items to a foreign national in the United States or posting non-public data to the internet.[66] However, software or data that is "published," i.e., "made available to the public without restrictions upon its further dissemination," is generally not subject to the EAR. Thus, the EAR generally cannot be used to restrict the publication or export of free and open-source software.[67]

The CCL currently contains a fairly broad set of export restrictions that require a license for exports to China of advanced semiconductor chips, input materials used in the fabrication of semiconductors, and semiconductor manufacturing equipment.[68] These restrictions are explicitly intended to "limit the PRC's ability to obtain advanced computing chips or further develop AI and 'supercomputer' capabilities for uses that are contrary to U.S. national security and foreign policy interests."[69] The CCL also currently restricts "neural computers"[70] and a narrowly-defined category of AI software useful for analysis of drone imagery[71]—"geospatial imagery 'software' 'specially designed' for training a Deep Convolutional Neural Network to automate the analysis of geospatial imagery and point clouds."[72]

---

[61] See 22 C.F.R. § 120.2; see 22 U.S.C. § 2278.
[62] See generally Bureau of Industry and Security, "Multilateral Export Control Regimes."
[63] See 15 C.F.R. § 730.3; see 50 U.S.C. §§ 4801–4852.
[64] See Supplement No. 1 to 15 CFR Part 774.
[65] 15 C.F.R. §§ 730.1, 730.7.
[66] 15 C.F.R. §§ 730.5, 774.
[67] 15 C.F.R. § 734.7; see generally Stav Zeitouni, "Milling the F/LOSS: Export Controls, Free and Open Source Software, and the Regulatory Future of the Internet," 23 N.Y.U. J. Legis. & Pub. Pol'y 905 (2021).
[68] See William A. Reinsch et al., "Optimizing Export Controls for Critical and Emerging Technologies," pp. 19–23. Center for Strategic and International Studies, May 2023.
[69] Bureau of Industry and Security, Department of Commerce, "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification," 87 FR 62186, 62187 (October 13, 2022).
[70] Bureau of Industry and Security. "Commerce Control List, Category 4." Department of Commerce, 2023.
[71] Dave Aitel, "We Need a Drastic Rethink on Export Controls for AI," Council on Foreign Relations, January 21, 2020.
[72] Bureau of Industry and Security, Department of Commerce, "Addition of Software Specially Designed To Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521 Series," 85 FR 459 (January 6, 2020).

In addition to the item-based CCL, the EAR include end-user controls, including an "Entity List" of individuals and companies subject to export licensing requirements.[73] Some existing end-user controls are designed to protect U.S. national security interests by hindering the ability of rivals like China to effectively conduct defense-relevant AI research. For example, in December 2022 BIS added a number of "major artificial intelligence (AI) chip research and development, manufacturing and sales entities" that "are, or have close ties to, government organizations that support the Chinese military and the defense industry" to the Entity List.[74]

The EAR also include, at 15 C.F.R. § 744, end-use based "catch-all" controls, which effectively prohibit the unlicensed export of items if the exporter knows or has reason to suspect that the item will be directly or indirectly used in the production, development, or use of missiles, certain types of drones, nuclear weapons, or chemical or biological weapons.[75] Section 744 also imposes a license requirement on the export of items which the exporter knows are intended for a military end use.[76]

Additionally, 15 C.F.R. § 744.6 requires "U.S. Persons" (a term which includes organizations as well as individuals) to obtain a license from BIS before "supporting" the design, development, production, or use of missiles or nuclear, biological, or chemical weapons, "supporting" the military intelligence operations of certain countries, or "supporting" the development or production of specified types of semiconductor chips in China. The EAR definition of "support" is extremely broad and covers "performing any contract, service, or employment you know may assist or benefit" the prohibited end uses in any way.[77]

For both the catch-all and U.S. Persons restrictions, BIS is authorized to send so-called "is informed" letters to individuals or companies advising that a given action requires a license because the action might result in a prohibited end-use or support a prohibited end-use or end-user.[78] This capability allows BIS to exercise a degree of control over exports and over the actions of U.S. Persons immediately, without going through the time-consuming process of Notice and Comment Rulemaking. For instance, BIS sent an "is informed" letter to NVIDIA on August 26, 2022, imposing a new license requirement on the export of certain chips to China and Russia, effective immediately, because BIS believed that there was a risk the chips would be used for military purposes.[79]

BIS has demonstrated a willingness to update its semiconductor export regime quickly and flexibly. For instance, after BIS restricted exports of AI-relevant chips in a rule issued on October 7, 2022, Nvidia modified its market-leading A100 and H100 chips to comply with the regulations and began to export the resultant modified A800 and H800 chips to China.[80] On October 17, 2023, BIS announced a new interim final rule prohibiting exports of A800 and H800 chips to China and waived the 30-day waiting period normally required by the Administrative Procedure Act so that the interim rule became effective just a few days after being

[73] Supplement no. 4 to 15 C.F.R. § 744.
[74] Bureau of Industry and Security, Department of Commerce, "Additions and Revisions to the Entity List and Conforming Removal From the Unverified List," 87 F.R. 77506 (December 19, 2022).
[75] See Emily S. Weinstein and Kevin Wolf, "For Export Controls on AI, Don't Forget the 'Catch-All' Basics," Center for Security and Emerging Technology (July 5, 2023).
[76] 15 C.F.R. § 744.21.
[77] 15 C.F.R. § 744.6(b)(6).
[78] 15 C.F.R. §§ 744.2(b), 744.3(b), 744.4(b), 744.6(c)(1).
[79] See NVIDIA Corporation SEC 8-K report, August 31, 2022; Leslie Glick, "BIS Restricts Semiconductor Exports to China: The New Rules and How They Unfolded," International Trade Blog, November 28, 2022.
[80] Benj Edwards, "US surprises Nvidia by speeding up new AI chip export ban." Ars Technica, October 24, 2023.

announced.[81] Commerce Secretary Gina Raimondo stated that "[i]f [semiconductor companies] redesign a chip around a particular cut line that enables them to do AI, I'm going to control it the very next day."[82]

In summation, the EAR currently impose a license requirement on a number of potentially dangerous actions relating to AI Hardware, Creation, and Proliferation. These controls have thus far been used primarily to restrict exports of AI hardware, but in theory they could also be used to impose licensing requirements on activities relating to AI creation and proliferation. The primary legal issue with this kind of regulation arises from the First Amendment.

Export controls and the First Amendment

Suppose that BIS determined that a certain AI model would be useful to terrorists or foreign state actors in the creation of biological weapons. Could BIS inform the developer of said model of this determination and prohibit the developer from making the model publicly available? Alternatively, could BIS add model weights which would be useful for training dangerous AI models to the CCL and require a license for their publication on the internet?

One potential objection to the regulations described above is that they would violate the First Amendment as unconstitutional prior restraints on speech. Courts have held that source code can be constitutionally protected expression, and in the 1990s export regulations prohibiting the publication of encryption software were struck down as unconstitutional prior restraints.[83] However, the question of when computer code constitutes protected expression is a subject of continuing scholarly debate,[84] and there is a great deal of uncertainty regarding the scope of the First Amendment's application to export controls of software and training data. The argument for restricting model weights may be stronger than the argument for restricting other relevant software or code items, because model weights are purely functional rather than communicative; they tell a computer what to do, but cannot be read or interpreted by humans.[85]

Currently, the EAR avoids First Amendment issues by allowing a substantial exception to existing licensing requirements for "published" information.[86] A great deal of core First Amendment communicative speech, such as basic research in universities, is "published" and therefore not subject to the EAR. Non-public proprietary software, however, can be placed on the CCL and restricted in much the same manner as tangible goods, usually without provoking any viable First Amendment objection.[87] Additionally, the EAR's recently added "U.S. Persons" controls regulate actions rather than directly regulating software, and it has been argued that this allows BIS to exercise some control over free and open source software without imposing an

[81] NVIDIA Corporation, SEC Filing (2023).
[82] Peter Martin, "We cannot let China get these chips': Commerce Secretary Raimondo says more funding needed for AI export controls." Fortune, December 2, 2023.
[83] See Bernstein v. United States Dept. of Justice, 176 F.3d 1132 (9th Cir. 1999).
[84] See, e.g., "First Amendment-Technology—Fifth Circuit Declines to Enjoin Regulation of Online Publication of 3D-Printing Files—Defense Distributed v. United States Department of State, 838 F.3d 451 (5th Cir. 2016)," 130 Harv. L. Rev. 1744 (2017) (arguing that CAD files used for the 3-D printing of firearms are not protected speech; discussing Fifth Circuit's refusal to enjoin ITAR restrictions on CAD files); Orin Kerr, "Are We Overprotecting Code? Thoughts on First-Generation Internet Law," 57 Wash. & Lee L. Rev. 1287 (2000).
[85] See Chris Byrd, *Export Controls for Open Source AI Model Weights*, presentation at CAIS AI Safety and Law Workshop, August 2023.
[86] 15 C.F.R. § 734.7.
[87] See Zeitouni, "Milling the F/LOSS," at 922–24; Roszel C. Thompson II, "Artificial Intelligence and Export Controls: Conceivable, But Counterproductive?," 22 J. Internet L. 1, 15 (discussing "attendant First Amendment issues" that would arise from export controls on open source software but do not apply to controls on proprietary software).

unconstitutional prior restraint, since under some circumstances providing access to an AI model may qualify as unlawful "support" for prohibited end-uses.[88]

Emergency powers

→ Applicable to: Tracking and Licensing AI Hardware & Creation; Licensing Proliferation
→ Already in use (IEEPA, to mandate know-your-customer requirements for IAAS providers pursuant to EO 14110); Unlikely to be used (§ 606(c))

The United States Code contains a number of statutes granting the President extraordinary powers that can only be used following the declaration of a national emergency. This section discusses two such emergency provisions—the International Emergency Economic Powers Act[89] and § 606(c) of the Communications Act of 1934[90]—and their existing and potential application to AI Oversight.

There are three existing statutory frameworks governing the declaration of emergencies: the National Emergencies Act ("NEA"),[91] the Robert T. Stafford Disaster Relief and Emergency Assistance Act,[92] and the Public Health Service Act.[93] Both of the authorities discussed in this section can be invoked following an emergency declaration under the NEA.[94] The NEA is a statutory framework that provides a procedure for declaring emergencies and imposes certain requirements and limitations on the exercise of emergency powers.[95]

International Emergency Economic Powers Act

The most frequently invoked emergency authority under U.S. law is the International Emergency Economic Powers Act ("IEEPA"), which grants the President expansive powers to regulate international commerce.[96] The IEEPA gives the President broad authority to impose a variety of economic sanctions on individuals and entities during a national emergency.[97] The IEEPA has been "the sole or primary statute invoked in 65 of the 71"[98] emergencies declared under the NEA since the NEA's enactment in 1976.

---

[88] For a thorough discussion of the First Amendment implications of export controls on AI models and model weights, see Doni Bloomfield, "Export Controls and Artificial Intelligence Biosecurity Risks" (March 21, 2024).
[89] 50 U.S.C. §§ 1701–1709.
[90] 47 U.S.C. § 151 *et seq.*
[91] 50 U.S.C. §§ 1601-1651.
[92] 42 U.S.C. §§ 5121-5207.
[93] 42 U.S.C. §§ 201-300mm–61.
[94] Comprehensive lists of Presidential emergency powers have been compiled by the Brennan Center and the Congressional Research Service.
[95] U.S. Congressional Research Service, "Emergency Authorities Under the NEA, Stafford Act, and PHSA," p. 3 (R46379; July 14, 2020). For instance, the NEA limits the duration of a national emergency to one year unless the President publishes a notice of renewal in the *Federal Register* and requires the President to specify the emergency authorities the President intends to invoke upon the declaration of a national emergency, publish any national emergency proclamation in the *Federal Register*, and maintain records of all rules and regulations promulgated pursuant to emergency powers. Ibid.
[96] See U.S. Congressional Research Service, "The International Emergency Economic Powers Act: Origins, Evolution, and Use," (R45618; March 25, 2022).
[97] U.S. Congressional Research Service, "The International Emergency Economic Powers Act: Origins, Evolution, and Use," p. 3 (R45618; March 20, 2019).
[98] Andrew Boyle, *Checking the President's Sanctions Powers: A Proposal to Reform the International Emergency Economic Powers Act*. Brennan Center for Justice, 2021.

The IEEPA authorizes the President to "investigate, regulate, or prohibit" transactions subject to U.S. jurisdiction that involve a foreign country or national.[99] The IEEPA also authorizes the investigation, regulation, or prohibition of any acquisition or transfer involving a foreign country or national.[100] The emergency must originate "in whole or in substantial part outside the United States" and must relate to "the national security, foreign policy, or economy of the United States."[101] There are some important exceptions to the IEEPA's general grant of authority—all "personal communications" as well as "information" and "informational materials" are outside of the IEEPA's scope.[102] The extent to which these protections would prevent the IEEPA from effectively being used for AI Oversight is unclear, because there is legal uncertainty as to whether, e.g., the transfer of AI model training weights overseas would be covered by one or more of the exceptions. If the relevant interpretive questions are resolved in a manner conducive to strict regulation, a partial licensing regime could be implemented under the IEEPA by making transactions contingent on safety and security evaluations. For example, foreign companies could be required to follow certain safety and security measures in order to offer subscriptions or sell an AI model in the U.S., or U.S.-based labs could be required to undergo safety evaluations prior to selling subscriptions to an AI service outside the country.

EO 14110 invoked the IEEPA to support §§ 4.2(c) and 4.2(d), provisions requiring the Department of Commerce to impose "Know Your Customer" ("KYC") reporting requirements on U.S. Infrastructure as a Service ("IAAS") providers. The emergency declaration justifying this use of the IEEPA originated in EO 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 1, 2015), which declared a national emergency relating to "malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States."[103] BIS introduced a proposed rule to implement the EO's KYC provisions on January 29, 2024.[104] The proposed rule would require U.S. IAAS providers (i.e., providers of cloud-based on-demand compute, storage, and networking services) to submit a report to BIS regarding any transaction with a foreign entity that could result in the training of an advanced and capable AI model that could be used for "malicious cyber-enabled activity."[105] Additionally, the rule would require each U.S. IAAS provider to develop and follow an internal "Customer Identification Program." Each Customer Identification Program would have to provide for verification of the identities of foreign customers, provide for collection and maintenance of certain information about foreign customers, and ensure that foreign resellers of the U.S. provider's IAAS products similarly verify, collect, and maintain.[106]

In short, the proposed rule is designed to allow BIS to track attempts at AI Creation by foreign entities who attempt to purchase the kinds of cloud compute resources required to train an advanced AI model, and to prevent such purchases from occurring. This tracking capability, if effectively implemented, would prevent foreign entities from circumventing export controls on AI Hardware by simply purchasing the computing power of advanced U.S. AI chips through the cloud.[107] The EO's use of the IEEPA has so far been considerably

[99] 50 U.S.C. § 1702(a)(1).
[100] Ibid.
[101] 50 U.S.C. § 1701.
[102] 50 U.S.C. § 1702(b)
[103] EO 13694, 80 FR 18077.
[104] Bureau of Industry and Security, Department of Commerce. "Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," 89 FR 5698 (January 29, 2024). The proposed rule will not go into effect until after the 90-day period for public comment and a subsequent period for BIS to respond to comments and make changes to the proposed rule have elapsed.
[105] Ibid. at 5706.
[106] See Brian J. Egan et al., "Know Your Cloud Customer: Commerce Department Proposes To Regulate Foreign Access to US IaaS Products." Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, February 13, 2024.
[107] See Janet Egan and Lennart Heim, "Oversight for Frontier AI through a Know-Your-Customer Scheme for Compute Providers." Center for the Governance of AI, October 25, 2023.

less controversial than the use of the DPA to impose reporting requirements on the creators of frontier models.[108]

Communications Act of 1934, § 606(c)

Section 606(c) of the Communications Act of 1934 could conceivably authorize a licensure program for AI Creation or Proliferation in an emergency by allowing the President to direct the closure or seizure of any networked computers or data centers used to run AI systems capable of aiding navigation. However, it is unclear whether courts would interpret the Act in such a way as to apply to AI systems, and any such use of Communications Act powers would be completely unprecedented. Therefore, § 606(c) is unlikely to be used for AI Oversight.

Section 606(c) confers emergency powers on the President "[u]pon proclamation by the President that there exists war or a … national emergency" if it is deemed "necessary in the interest of national security or defense." The National Emergency Act ("NEA") of 1976 governs the declaration of a national emergency and established requirements for accountability and reporting during emergencies.[109] Neither statute defines "national emergency." In an emergency, the President may (1) "suspend or amend … regulations applicable to … stations or devices capable of emitting electromagnetic radiations"; (2) close "any station for radio communication, or any device capable of emitting electromagnetic radiations between 10 kilocycles and 100,000 megacycles [10 kHz–100 GHz], which is suitable for use as a navigational aid beyond five miles" and (3) authorize "use or control" of the same.[110]

In other words, § 606(c) empowers the President to seize or shut down certain types of electronic "device" during a national emergency. The applicable definition of "device" could arguably encompass most of the computers, servers, and data centers utilized in AI Creation and Proliferation.[111] Theoretically, § 606(c) could be invoked to sanction seizure or closure of these devices. However, § 606(c) has never been utilized, and there is significant uncertainty concerning whether courts would allow its application to implement a comprehensive program of AI oversight.

Federal funding conditions

- → Potentially applicable to: Tracking and Licensing AI Hardware & AI Creation; Licensing AI Proliferation
- → Reasonably likely to be used for Oversight in some capacity

---

[108] There are a number of factors that likely contribute to the general acceptance (so far) of the KYC requirements. For one thing, the President has greater legal authority to act without authorization from Congress in matters involving foreign actors. For another, President Trump previously invoked the IEEPA in a similar manner in EO 13984 (January 19 2021), an anti-cybercrime order which EO 14110 references and uses as a jumping-off point for new, AI-specific KYC requirements. And perhaps most importantly, the issue of preventing China from obtaining advanced AI systems is, unlike domestic AI governance, a locus of strong bipartisan consensus.

[109] 50 USC § 1601-51.

[110] 47 USC § 606(c).

[111] The statute's definition of "device" technically encompasses many modern computers accessing or running AI systems during AI Creation and Proliferation, as they are devices capable of emitting electromagnetic radiation in the relevant range that can be used as navigational aids. However, some modern servers or data centers employed to train AI may not fall within the ambit of § 606(c) because they transmit and receive data through optical fiber cable. Future devices surpassing the 100 GHz maximum would similarly not be covered.

Attaching conditions intended to promote AI safety to federal grants and contracts could be an effective way of creating a partial licensing regime for AI Creation and Proliferation. Such a regime could be circumvented by simply forgoing federal funding, but could still contribute to an effective overall scheme for Oversight.

Funding conditions for federal grants and contracts

Under the Federal Property and Administrative Services Act, also known as the Procurement Act,[112] the President can "prescribe policies and directives" for government procurement, including via executive order.[113] Generally, courts have found that the President may order agencies to attach conditions to federal contracts so long as a "reasonably close nexus"[114] exists between the executive order and the Procurement Act's purpose, which is to provide an "economical and efficient system" for procurement.[115] This is a "lenient standard",[116] and it is likely that an executive order directing agencies to include conditions intended to promote AI safety in all AI-related federal contracts would be upheld under it.

Presidential authority to impose a similar condition on AI-related federal grants via executive order is less clear. Generally, "the ability to place conditions on federal grants ultimately comes from the Spending Clause, which empowers Congress, not the Executive, to spend for the general welfare."[117] It is therefore likely that any conditions imposed on federal grants will be imposed by legislation rather than by executive order. However, plausible arguments for Presidential authority to impose grant conditions via executive order in certain circumstances do exist, and even in the absence of an explicit condition executive agencies often wield substantial discretion in administering grant programs.[118]

Implementation of federal contract conditions

Government-wide procurement policies are set by the Federal Acquisition Regulation ("FAR"), which is maintained by the Office of Federal Procurement Policy ("OFPP").[119] A number of FAR regulations require the insertion of a specified clause into all contracts of a certain type; for example, FAR § 23.804 requires the insertion of clauses imposing detailed reporting and tracking requirements for ozone-depleting chemicals into all federal contracts for refrigerators, air conditioners, and similar goods.[120] Amending the FAR to include a clause imposing regulations related to the safe development of AI and prohibiting the publication of any sufficiently advanced model that had not been reviewed and deemed safe in accordance with specified procedures would effectively impose a licensing requirement on AI Creation and Proliferation, albeit a requirement that would apply only to entities receiving government funding.

---

[112] 40 U.S.C. § 101 *et seq.*
[113] 40 U.S.C. § 121(a).
[114] See U.S. Congressional Research Service, "Presidential Authority to Impose Requirements on Federal Contractors," p. 15 (R41866; June 14, 2011).
[115] 40 U.S.C. § 101(a).
[116] *UAW-Labor Employment and Training v. Chao*, 325 F.3d 360, 367 (D.C. Cir. 2003).
[117] *Texas Educ. Agency v. United States Dep't of Educ.*, 992 F.3d 350, 362 (5th Cir. 2021); see also *City of San Francisco v. Trump*, 897 F.3d 1225, 1233-34 (9th Cir. 2018) (striking down executive order that sought to deprive "sanctuary jurisdictions" of federal grant funding because Congress appropriated the funds in question and "ha[d] not delegated authority to the Executive to condition new grants" on compliance with federal immigration law).
[118] See 2 C.F.R. § 200.206(b)(2)(v) (directing agencies awarding discretionary grants to consider "[t]he applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on non-Federal entities").
[119] U.S. Congressional Research Service, "Office of Management and Budget (OMB): An Overview," p. 22 (RS21665; June 22, 2023).
[120] Federal Acquisition Regulation § 23.804.

A less ambitious real-life approach to implementing federal contract conditions encouraging the safe development of AI under existing authorities appears in Executive Order 14110. Section 4.4(b) of that EO directs the White House Office of Science and Technology Policy (OSTP) to release a framework designed to encourage DNA synthesis companies to screen their customers, in order to reduce the danger of e.g. terrorist organizations acquiring the tools necessary to synthesize biological weapons.[121] Recipients of federal research funding will be required to adhere to the OSTP's Framework, which was released in April 2024.[122]

Potential scope of oversight via conditions on federal funding

Depending on their nature and scope, conditions imposed on grants and contracts could facilitate the tracking and/or licensing of AI Hardware, Creation, and Proliferation. The conditions could, for example, specify best practices to follow during AI Creation, and prohibit labs that accepted federal funds from developing frontier models without observing said practices; this, in effect, would create a non-universally applicable licensing regime for AI Creation. The conditions could also specify procedures (e.g. audits by third-party or government experts) for certifying that a given model could safely be made public, and prohibit the release of any AI model developed using a sufficiently large training run until it was so certified. For Hardware, the conditions could require contractors and grantees to track any purchase or sale of the relevant chips and chipmaking equipment and report all such transactions to a specified government office.

The major limitation of Oversight via federal funding conditions is that the conditions might not apply to entities that did not receive funding from the federal government. However, it is possible that this regulatory gap could be at least partially closed by drafting the included conditions to prohibit contractors and grantees from contracting with companies that fail to abide by some or all of the conditions. This would be a novel and aggressive use of federal funding conditions, but would likely hold up in court.

FTC consumer protection authorities

- → Applicable to: Tracking and Licensing AI Creation, Licensing AI Proliferation
- → Unlikely to be used for licensing, but somewhat likely to be involved in tracking AI Creation in some capacity

The Federal Trade Commission Act ("FTC Act") includes broad consumer protection authorities, two of which are identified in this section as being potentially relevant to AI Oversight. Under § 5 of the FTC Act, the Federal Trade Commission ("FTC") can pursue enforcement actions in response to "unfair or deceptive acts or practices in or affecting commerce"[123]; this authority could be relevant to licensing for AI creation and proliferation. And under § 6(b), the FTC can conduct industry studies that could be useful for tracking AI creation.

The traditional test for whether a practice is "unfair," codified at § 5(n), asks whether the practice: (1) "causes or is likely to cause substantial injury to consumers" (2) which is "not reasonably avoidable by consumers themselves" and (3) is not "outweighed by countervailing benefits to consumers or to competition."[124]

---

[121] EO 14110 at § 4.4(b).
[122] See Fast Track Action Committee on Synthetic Nucleic Acid Procurement Screening, "Framework for Nucleic Acid Synthesis Screening" (April 2024).
[123] 15 U.S.C. § 45.
[124] 15 U.S.C. § 45(n); see *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243–246 (3d Cir. 2015).

"Deceptive" practices have been defined as involving: (1) a representation, omission, or practice, (2) that is material, and (3) that is "likely to mislead consumers acting reasonably under the circumstances."[125]

FTC Act § 5 oversight

Many potentially problematic or dangerous applications of highly capable LLMs would involve "unfair or deceptive acts or practices" under § 5. For example, AI safety researchers have warned of emerging risks from frontier models capable of "producing and propagating highly persuasive, individually tailored, multi-modal disinformation."[126] A commercially available model with such capabilities would likely constitute a violation of § 5's "deceptive practices" prong.[127]

Furthermore, the FTC has in recent decades adopted a broad plain-meaning interpretation of the "unfair practices" prong, meaning that irresponsible AI development practices that impose risks on consumers could constitute an "unfair practice."[128] The FTC has recently conducted a litigation campaign to impose federal data security regulation via § 5 lawsuits, and this campaign could serve as a model for a future effort to require AI labs to implement AI safety best practices while developing and publishing frontier models.[129] In its data security lawsuits, the FTC argued that § 5's prohibition of unfair practices imposed a duty on companies to implement reasonable data security measures to protect their consumers' data.[130] The vast majority of the FTC's data security cases ended in settlements that required the defendants to implement certain security best practices and agree to third party compliance audits.[131] Furthermore, in several noteworthy data security cases, the FTC has reached settlements under which defendant companies have been required to delete models developed using illegally collected data.[132]

The FTC can bring § 5 claims based on prospective or "likely" harms to consumers.[133] And § 5 can be enforced against defendants whose conduct is not the most proximate cause of an injury, such as an AI lab whose product is foreseeably misused by criminals to deceive or harm consumers, when the defendant

---

[125] *F.T.C. v. Stefanchik*, 559 F.3d 924, 928 (9th Cir. 2009). Recent FTC guidance states that the use of AI "model[s] that cause more harm than good" constitutes an unfair practice under § 5. Elisa Jillson, "Aiming for truth, fairness, and equity in your company's use of AI." FTC Business Blog (April 9, 2021). However, it is doubtful whether a court would accept such a broad interpretation of the FTC's § 5 authority.

[126] Markus Anderljung et al., *Frontier AI Regulation: Managing Emerging Risks to Public Safety*, p. 7. arXiv:2307.03718 (July 11, 2023).

[127] See Michael Atleson, "Chatbots, deepfakes, and voice clones: AI deception for sale." FTC Business Blog (March 20, 2023) ("The FTC Act's prohibition on deceptive or unfair conduct can apply if you make, sell, or use a tool that is effectively designed to deceive – even if that's not its intended or sole purpose.").

[128] Tyler Becker, *When Congress Makes No Policy Choice: The Case of FTC Data Security Enforcement*, 120 Colum. L. Rev. F. 134 (2020).

[129] Ibid.

[130] Ibid.

[131] See, e.g., Avi Gesser et al., *Model Destruction - The FTC's Powerful New AI and Privacy Enforcement Tool*. Debevoise & Plimpton Data Blog, March 22, 2022.

[132] See Final Order, *In re Cambridge Analytica LLC*, FTC Docket No. 9383 (Nov. 25, 2019); Decision, *In re Everalbum, Inc.*, FTC Docket No. C-4743 (May 6, 2021); Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief, *U.S. v. Kurbo Inc.*, 3:22-cv-00946 (N.D. Cal. March 3, 2022); see also Rebecca Kelly Slaughter, Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission, pp. 39–40, Yale Journal of Law and Technology (2021) (discussing "algorithmic disgorgement," i.e., a remedy pursuant to which models or algorithms developed using illegally collected data are deleted).

[133] See *Wyndham Worldwide*, 799 F.3d at 246 (noting that "the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs").

provided others with "the means and instrumentalities for the commission of deceptive acts or practices."[134] Thus, if courts are willing to accept that the commercial release of models developed without observation of AI safety best practices is an "unfair" or "deceptive" act or practice under § 5, the FTC could impose, on a case-by-case basis,[135] something resembling a licensing regime addressing areas of AI creation and proliferation. As in the data security settlements, the FTC could attempt to reach settlements with AI labs requiring the implementation of security best practices and third party compliance audits, as well as the deletion of models created in violation of § 5. This would not be an effective permanent substitute for a formal licensing regime, but could function as a stop-gap measure in the short term.

FTC industry studies

Section 6(b) of the FTC Act authorizes the conduct of industry studies.[136] The FTC has the authority to collect confidential business information to inform these studies, requiring companies to disclose information even in the absence of any allegation of wrongdoing. This capability could be useful for tracking AI Creation.

Limitations of FTC oversight authority

The FTC has already signaled that it intends to "vigorously enforce" § 5 against companies that use AI models to automate decisionmaking in a way that results in discrimination on the basis of race or other protected characteristics.[137] Existing guidance also shows that the FTC is interested in pursuing enforcement actions against companies that use LLMs to deceive consumers.[138] The agency has already concluded a few successful § 5 enforcement actions targeting companies that used (non-frontier) AI models to operate fake social media accounts and deceptive chatbots.[139] And in August 2023 the FTC brought a § 5 "deceptive acts or practices" enforcement action alleging that a company named Automators LLC had deceived customers with exaggerated and untrue claims about the effectiveness of the AI tools it used, including the use of ChatGPT to create customer service scripts.[140]

Thus far, however, there is little indication that the FTC is inclined to take on broader regulatory responsibilities with respect to AI safety. The § 5 prohibition on "unfair practices" has traditionally been used for consumer protection, and commentators have suggested that it would be an "awkward tool" for addressing more serious national-security-related AI risk scenarios such as weapons development, which the FTC has not

[134] Complaint for Permanent Injunction and Other Equitable Relief, *FTC v. Devumi, LLC*, No. 19-cv-81419 (S.D. Fla. Oct. 18, 2019) (alleging that provider of automated social media accounts provided its clients with "the means and instrumentalities for the commission of deceptive acts or practices."); see *Wyndham Worldwide*, 799 F.3d at 246 (citing Restatement (Second) of Torts § 449 (1965)).
[135] Or, if the FTC successfully "argue[s] that inadequate controls are a common industry practice," via a generally applicable prohibitory trade rule. *FTC Authority to Regulate Generative AI*. Note that, under 15 USC § 57a, the FTC is authorized to promulgate "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce."
[136] 15 U.S.C. § 46(b); see Federal Trade Commission, "Patent Assertion Entity Activity - An FTC Study" (October 2016).
[137] Federal Trade Commission, "FTC Chair Khan and Officials from DOJ, CFPB and EEOC Release Joint Statement on AI." April 25, 2023; see Slaughter, *Algorithms and Economic Justice*. The FTC can also bring enforcement actions under the Fair Credit Reporting Act and the Equal Credit Opportunity Act. Recent FTC guidance advises AI companies that it will bring FRCA and ECOA enforcement actions against companies that use AI in a way that results in credit discrimination or discriminatory denial of employment, housing, credit, or insurance benefits. See Jillson, "Aiming for truth, fairness, and equity."
[138] See Atleson, "Chatbots, deepfakes, and voice clones."
[139] See, e.g., FTC v. Devumi, LLC.
[140] Complaint, *FTC v. Automators LLC*, No. 23-cv-1444 (S.D. Cal. August 8, 2023)

traditionally dealt with.[141] Moreover, even if the FTC were inclined to pursue an aggressive AI Oversight agenda, the agency's increasingly politically divisive reputation might contribute to political polarization around the issue of AI safety and inhibit bipartisan regulatory and legislative efforts.

Committee on Foreign Investment in the United States

→ Potentially applicable to: Tracking and/or Licensing AI Hardware and Creation
→ Unlikely to be used to directly track or license frontier AI models, but could help to facilitate effective Oversight.

The Committee on Foreign Investment in the United States ("CFIUS") is an interagency committee charged with reviewing certain foreign investments in U.S. businesses or real estate and with mitigating the national security risks created by such transactions.[142] If CFIUS determines that a given investment threatens national security, CFIUS can recommend that the President block or unwind the transaction.[143] Since 2012, Presidents have blocked six transactions at the recommendation of CFIUS, all of which involved an attempt by a Chinese investor to acquire a U.S. company (or, in one instance, U.S.-held shares of a German company).[144] In three of the six blocked transactions, the company targeted for acquisition was a semiconductor company or a producer of semiconductor manufacturing equipment.[145]

Congress expanded CFIUS's scope and jurisdiction in 2018 by enacting the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA").[146] FIRRMA was enacted in part because of a Pentagon report warning that China was circumventing CFIUS by acquiring minority stakes in U.S. startups working on "critical future technologies" including artificial intelligence.[147] This, the report warned, could lead to large-scale technology transfers from the U.S. to China, which would negatively impact the economy and national security of the U.S.[148] Before FIRRMA, CFIUS could only review investments that might result in at least partial foreign control of a U.S. business.[149] Under Department of the Treasury regulations implementing FIRRMA, CFIUS can now review "any direct or indirect, non-controlling foreign investment in a U.S. business producing or developing critical technology."[150] President Biden specifically identified artificial intelligence as a "critical technology" under FIRRMA in Executive Order 14083.[151]

CFIUS imposes, in effect, a licensing requirement for foreign investment in companies working on AI Hardware and AI Creation. It also facilitates tracking of AI Hardware and Creation, since it reduces the risk of

[141] Ibid.
[142] 31 C.F.R. § 800.101(a). Many of CFIUS's authorities come from Title VII of the Defense Production Act, but CFIUS is "generally considered separate and distinct from the DPA." U.S. Congressional Research Service, "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," p. 1 (R43767; October 6, 2023).
[143] 50 U.S.C. § 4565(l)(2).
[144] U.S. Congressional Research Service, "The Committee on Foreign Investment in the United States," p. 2 (IF10177; August 3, 2023).
[145] Fischer *et al.*, "AI Policy Levers," p. 20.
[146] Ibid.
[147] Michael Brown and Pavneet Singh, "How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," p. 3 (Defense Innovation Unit Experimental 2018); see Fischer *et al.*, "AI Policy Levers," p. 20.
[148] Brown and Singh, "Chinese Investments in Emerging Technology," p. 3.
[149] John M. Beahn *et al.*, "Final CFIUS Regulations Implement Significant Changes by Broadening Jurisdiction and Updating Scope of Reviews," Shearman & Sterling, January 14, 2020.
[150] Ibid.
[151] Executive Order 14083, "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States," 87 F.R. 57369 (September 15, 2022).

cutting-edge American advances, subject to American Oversight, being clandestinely transferred to countries in which U.S. Oversight of any kind is impossible. A major goal of any AI Oversight regime will be to stymie attempts by foreign adversaries like China and Russia to acquire U.S. AI capabilities, and CFIUS (along with export controls) will play a major role in the U.S. government's pursuit of this goal.

Atomic Energy Act

→ Applicable to: Licensing AI Creation and Proliferation
→ Somewhat unlikely to be used to create a licensing regime in the absence of new legislation

The Atomic Energy Act ("AEA") governs the development and regulation of nuclear materials and information. The AEA prohibits the disclosure of "Restricted Data," which phrase is defined to include all data concerning the "design, manufacture, or utilization of atomic weapons."[152] The AEA also prohibits communication, transmission, or disclosure of any "information involving or incorporating Restricted Data" when there is "reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation." A sufficiently advanced frontier model, even one not specifically designed to produce information relating to nuclear weapons, might be capable of producing Restricted Data based on inferences from or analysis of publicly available information.[153]

A permitting system that regulates access to Restricted Data already exists.[154] Additionally, the Attorney General can seek a prospective court-ordered injunction against any "acts or practices" that the Department of Energy ("DOE") believes will violate the AEA.[155] Thus, licensing AI Creation and Proliferation under the AEA could be accomplished by promulgating DOE regulations stating that AI models that do not meet specified safety criteria are, in DOE's judgment, likely to be capable of producing Restricted Data and therefore subject to the permitting requirements of 10 C.F.R. § 725.

However, there are a number of potential legal issues that make the application of the AEA to AI Oversight unlikely. For instance, there might be meritorious First Amendment challenges to the constitutionality of the AEA itself or to the licensing regime proposed above, which could be deemed a prior restraint of speech.[156] Or, it might prove difficult to establish beforehand that an AI lab had "reason to believe" that a frontier model would be used to harm the U.S. or to secure an advantage for a foreign state.[157]

---

[152] 42 U.S.C. § 2014(y).
[153] Frontier AI systems have in the past years proved capable of generating novel toxic molecules, predicting the existence of new thermoelectric materials, and rederiving certain laws of physics from raw video data.
[154] See 10 C.F.R. § 725.
[155] 42 U.S.C. § 2280.
[156] See *United States v. The Progressive*, 467 F. Supp. 990 (W.D. Wis. 1979), in which the government sought to enjoin publication of information relating to the design of hydrogen bombs. The data in question was compiled from publicly available sources, and while the district court initially agreed to issue an injunction, the government ultimately dropped its case before the district court decision could be reviewed by a federal appellate court. Ibid. There is generally a strong presumption under U.S. law against "prior restraints" on speech. See *New York Times v. United States*, 403 U.S. 713, 725-27 (1971).
[157] See 42 U.S.C. § 2274(b).

Copyright law

→ Potentially applicable to: Licensing AI Creation and Proliferation
→ Unlikely to be used directly for Oversight, but will likely indirectly affect Oversight efforts

Intellectual property ("IP") law will undoubtedly play a key role in the future development and regulation of generative AI. IP's role in AI Oversight, narrowly understood, is more limited. That said, there are low-probability scenarios in which IP law could contribute to an ad hoc licensing regime for frontier AI models. This section discusses the possibility that U.S. Copyright law[158] could contribute to a sort of licensing regime for frontier AI models.

In September and October 2023, OpenAI was named as a defendant in a number of recent putative class action copyright lawsuits.[159] The complaints in these suits allege that OpenAI trained GPT-3. GPT-3.5, and GPT-4 on datasets including hundreds of thousands of pirated books downloaded from a digital repository like Z-Library or LibGen.[160] In December 2023, the New York Times filed a copyright lawsuit against OpenAI and Microsoft alleging that OpenAI infringed its copyrights by using Times articles in its training datasets.[161] The Times also claimed that GPT-4 had "memorized" long sections of copyrighted articles and could "recite large portions of [them] verbatim" with "minimal prompting."[162]

The eventual outcome of these lawsuits is uncertain. Some commentators have suggested that the infringement case against OpenAI is strong and that the use of copyrighted material in a training run is copyright infringement.[163] Others have suggested that using copyrighted work for an LLM training run falls under fair use, if it implicates copyright law at all, because training a model on works meant for human consumption is a transformative use.[164]

In a worst-case scenario for AI labs, however, a loss in court could in theory result in an injunction prohibiting OpenAI from using copyrighted works in its training runs and statutory damages of up to $150,000 per copyrighted work infringed.[165] The dataset that OpenAI is alleged to have used to train GPT-3, GPT-3.5, and GPT-4 contains over a 100,000 copyrighted works,[166] meaning that the upper bound for potential statutory damages for OpenAI any other AI lab that used the same dataset to train a frontier model would be upwards of $15 billion.

Such a decision would have a significant impact on the development of frontier LLMs in the United States. The amount of text required to train a cutting-edge LLM is such that an injunction requiring OpenAI and its

[158] See 17 U.S.C. §§ 101 *et seq.*
[159] See Complaint, *Authors Guild v. OpenAI Inc*, 23-cv-8292 (S.D.N.Y. September 19, 2023); Complaint, *Chabon v. OpenAI Inc*, 3:23-cv-04625 (N.D. Cal. September 8, 2023); Complaint, *Tremblay v. OpenAI Inc*, 3:23-cv-03223 (N.D. Cal.); Complaint, *Silverman v. OpenAI Inc*, 3:23-cv-03416 (N.D. Cal.).
[160] Complaint, *Authors Guild v. OpenAI Inc*, at pp. 12–14.
[161] Complaint, *The New York Times Company v. Microsoft*, 23-cv-11195 (S.D.N.Y. December 27, 2023), at pp. 160–162.
[162] Ibid. at p. 99.
[163] See New York Times, September 20, 2023, "Franzen, Grisham and Other Prominent Authors Sue OpenAI" (quoting a copyright law expert asserting that "courts are going to say that copying into the database is an infringement in itself").
[164] See Van Lindberg, "Building and Using Generative Models Under U.S. Copyright Law," 18 Rutgers Bus. L. Rev. 1 (2023); OpenAI, "Comment Regarding Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation," PTO-C-2019-0038.
[165] See Complaint, *Authors Guild v. OpenAI Inc*, at p. 47; 17 U.S.C. §§ 502, 504.
[166] See Kate Knibbs, The Battle Over Books3 Could Change AI Forever, Wired (Sept. 4, 2023).

competitors to train their models without the use of any copyrighted material would require the labs to retool their approach to training runs.

Given the U.S. government's stated commitment to maintaining U.S. leadership in Artificial Intelligence,[167] it is unlikely that Congress would allow such a decision to inhibit the development of LLMs in the United States on anything resembling a permanent basis. But copyright law could in theory impose, however briefly, a *de facto* halt on large training runs in the United States. If this occurred, the necessity of Congressional intervention[168] would create a natural opportunity for imposing a licensing requirement on AI Creation.

Antitrust authorities

- → Applicable to: Tracking and Licensing AI Hardware and AI Creation
- → Unlikely to be used directly for government tracking or licensing regimes, but could facilitate the creation of an imperfect private substitute for true Oversight

U.S. antitrust authorities include the Sherman Antitrust Act of 1890[169] and § 5 of the FTC Act,[170] both of which prohibit anticompetitive conduct that harms consumers. The Sherman Act is enforced primarily by the Department of Justice's ("DOJ") Antitrust Division, while § 5 of the FTC Act is enforced by the FTC.

This section focuses on a scenario in which non-enforcement of antitrust law under certain circumstances could facilitate the creation of a system of voluntary agreements between leading AI labs as an imperfect and temporary substitute for a governmental Oversight regime. As discussed above in Section 1, one promising short-term option to ensure the safe development of frontier models prior to the enactment of comprehensive Oversight legislation is for leading AI labs to enter into voluntary agreements to abide by responsible AI development practices. In the absence of cooperation, "harmful race dynamics" can develop in which the winner-take-all nature of a race to develop a valuable new technology can incentivize firms to disregard safety, transparency, and accountability.[171]

A large number of voluntary agreements have been proposed, notably including the "Assist Clause" in OpenAI's charter. The Assist Clause states that, in order to avoid "late-stage AGI development becoming a competitive race without time for adequate safety precautions," OpenAI commits to "stop competing with and start assisting" any safety-conscious project that comes close to building Artificial General Intelligence before OpenAI does.[172] Other potentially useful voluntary agreements include agreements to: (1) abide by shared safety standards, (2) engage in joint AI safety research ventures, (3) share information, including by mutual monitoring, sharing reports about incidents during safety testing, and comprehensively accounting for compute usage,[173] (4) pause or set an agreed pace for increases in the size of training runs for frontier AI models, and/or

---

[167] See, e.g., 15 U.S.C. § 9411(a).
[168] Perhaps in the form of a legislative safe harbor from copyright law for LLM training runs similar to the safe harbors that currently exist under UK and German copyright law. See Urheberrechts-Wissensgesellschafts-Gesetz [Law on Copyright and Related Rights], Sep. 7, 2017, RGBl I at 3346 (Ger.) (English translation); Copyrights, Designs and Patents Act, (1988) § 29A(1) (UK).
[169] 15 U.S.C. § 1–7.
[170] 15 U.S.C. § 45.
[171] See S.-S. Hua and H. Belfield, "AI & antitrust: Reconciling tensions between competition law and cooperative AI development," 23 Yale Journal of Law & Technology 415, 431 (2021).
[172] OpenAI Charter.
[173] Hua and Belfield, "AI & antitrust," at 491–506.

(5) pause specified research and development activities for all labs whenever one lab develops a model that exhibits dangerous capabilities.[174]

Universal, government-administered regimes for tracking and licensing AI Hardware, Creation, and Proliferation would be preferable to the voluntary agreements described for a number of reasons, notably including ease of enforcement and a lack of economic incentives for companies to defect and refuse to agree. However, many of the proposed agreements could accomplish some of the goals of AI Oversight. Compute accounting, for example, would be a substitute (albeit an imperfect one) for comprehensive tracking of AI Hardware, and other information-sharing agreements would be imperfect substitutes for tracking AI Creation. Agreements to cooperatively pause upon discovery of dangerous capabilities would serve as an imperfect substitute for an AI Proliferation licensing regime. Agreements to abide by shared safety standards would substitute for an AI Creation licensing regime, although the voluntary nature of such an arrangement would to some extent defeat the point of a licensing regime.

All of the agreements proposed, however, raise potential antitrust concerns. OpenAI's Assist Clause, for example, could accurately be described as an agreement to restrict competition,[175] as could cooperative pausing agreements.[176] Information-sharing agreements between competitors can also constitute antitrust violations, depending on the nature of the information shared and the purpose for which competitors share it.[177] DOJ or FTC enforcement proceedings against AI companies over such voluntary agreements —or even uncertainty regarding the possibility of such enforcement actions— could deter AI labs from implementing a system for partial self-Oversight.

One option for addressing such antitrust concerns would be the use of § 708 of the DPA, discussed above in Section 1, to officially sanction voluntary agreements between companies that might otherwise violate antitrust laws. Alternatively, the FTC and the DOJ could publish guidance informing AI labs of their respective positions on whether and under what circumstances a given type of voluntary agreement could constitute an antitrust violation.[178] In the absence of some sort of guidance or safe harbor, the risk-averse in-house legal teams at leading AI companies (some of which are presently involved in and/or staring down the barrel of ultra-high-stakes antitrust litigation[179]) are unlikely to allow any significant cooperation or communication between rank and file employees.

There is significant historical precedent for national security concerns playing a role in antitrust decisions.[180] Most recently, after the FTC secured a permanent injunction to prohibit what it viewed as anticompetitive conduct from semiconductor company Qualcomm, the DOJ filed an appellate brief in support of Qualcomm

[174] See Jide Alaga & Jonas Schuett, "Coordinated Pausing," arXiv:2310.00374, p. 3 (Centre for the Governance of AI, 2023).
[175] See Hua and Belfield, "AI & antitrust," at 455–482 (discussing antitrust implications of Assist Clause in the context of European competition law and potential strategies to mitigate antitrust risk).
[176] See Alaga & Schuett, "Coordinated Pausing," at 15 (discussing concern that voluntary coordinated pausing agreements could violate US antitrust laws and potential strategies to mitigate antitrust risk).
[177] See generally Corby C. Anderson and Ted P. Pearce, "The Antitrust Risks of Information Sharing," 23 Franchise L.J. 17 (2003).
[178] See "Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information" (April 10, 2014) (explaining that FTC and DOJ "do not believe that antitrust is – or should be – a roadblock to legitimate cybersecurity information sharing").
[179] See Nico Grant, "Google's Antitrust Loss to Epic Could Preview Its Legal Fate in 2024," *New York Times* (December 12, 2023); Jan Wolfe, "Big Tech Braces for a Wave of Antitrust Rulings in 2024," *Wall Street Journal* (January 1, 2024).
[180] See generally Cullen O'Keefe, "How Will National Security Considerations Affect Antitrust Decisions in AI? An Examination of Historical Precedents" (Centre for the Governance of AI, 2021).

and in opposition to the FTC, arguing that the injunction would "significantly impact U.S. national security" and incorporating a statement from a DOD official to the same effect.[181] The Ninth Circuit sided with Qualcomm and the DOJ, citing national security concerns in an order granting a stay[182] and later vacating the injunction.[183]

Biological Weapons Anti-Terrorism Act; Chemical Weapons Convention Implementation Act

→ Potentially applicable to: Licensing AI Creation & Proliferation
→ Unlikely to be used for AI oversight

Among the most pressing dangers posed by frontier AI models is the risk that sufficiently capable models will allow criminal or terrorist organizations or individuals to easily synthesize dangerous biological or chemical agents or to easily design and synthesize novel and catastrophically dangerous biological or chemical agents for use as weapons.[184] The primary existing U.S. government authorities prohibiting the development and acquisition of biological and chemical weapons are the Biological Weapons Anti-Terrorism Act of 1989 ("BWATA")[185] and the Chemical Weapons Convention Implementation Act of 1998 ("CWCIA"),[186] respectively.

The BWATA implements the Biological Weapons Convention ("BWC"), a multilateral international agreement that prohibits the development, production, acquisition, transfer, and stockpiling of biological weapons.[187] The BWC requires, *inter alia*, that states parties implement "any necessary measures" to prevent the proliferation of biological weapons within their territorial jurisdictions.[188] In order to accomplish this purpose, Section 175(a) of the BWATA prohibits "knowingly develop[ing], produc[ing], stockpil[ing], transfer[ing], acquir[ing], retain[ing], or possess[ing]" any "biological agent," "toxin," or "delivery system" for use as a weapon, "knowingly assist[ing] a foreign state or any organization" to do the same, or "attempt[ing], threaten[ing], or conspir[ing]" to do either of the above.[189] Under § 177, the Government can file a civil suit to enjoin the conduct prohibited in § 175(a).[190]

---

[181] Ibid.
[182] *Fed. Trade Comm'n v. Qualcomm Inc.*, 935 F.3d 752, 756 (9th Cir. 2019).
[183] *Fed. Trade Comm'n v. Qualcomm Inc.*, 969 F.3d 974 (9th Cir. 2020).
[184] See Markus Anderljung et al., *Frontier AI Regulation: Managing Emerging Risks to Public Safety*, p. 7, arXiv:2307.03718 (July 11, 2023); Daniil A. Boiko *et al.*, "Emergent autonomous scientific research capabilities of large language models," arXiv:2304.05332 (April 2023); Fabio Urbina *et al.*, "Dual use of artificial-intelligence- powered drug discovery," Nature Machine Intelligence 4.3 (Mar. 2022), pp. 189–191; "Final Report" (National Security Commission on Artificial Intelligence, March 2021), pp. 52–53.
[185] Pub. L. 101-298, 104 Stat. 201, codified as amended at 18 U.S.C. § 175 *et seq.*
[186] Pub. L. 105-277, 112 Stat. 2681–856, as amended.
[187] Piers Millett, "The Biological Weapons Convention: Securing Biology in the Twenty-First Century," Journal of Conflict & Security Law 15 (2010), at 25.
[188] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxic Weapons and on Their Destruction (the "Biological Weapons Convention"), opened for signature Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163 (entered into force Mar. 26, 1975).
[189] 18 U.S.C. § 175(a).
[190] 18 U.S.C. § 177.

The CWCIA implements the international Convention on the Prohibition of the Development, Stockpiling, and Use of Chemical Weapons and on Their Destruction.[191] Under the CWCIA it is illegal for a person to "knowingly develop, produce, otherwise acquire, transfer directly or indirectly, receive, stockpile, retain, own, possess, or use, or threaten to use, any chemical weapon," or to "assist or induce, in any way, any person to" do the same.[192] Under § 229D, the Government can file a civil suit to enjoin the conduct prohibited in § 229 or "the preparation or solicitation to engage in conduct prohibited under § 229."[193]

It could be argued that publicly releasing an AI model that would be a useful tool for the development or production of biological or chemical weapons would amount to "knowingly assist[ing]" (or attempting or conspiring to knowingly assist) in the development of said weapons, under certain circumstances. Alternatively, with respect to chemical weapons, it could be argued that the creation or proliferation of such a model would amount to "preparation" to knowingly assist in the development of said weapons. If these arguments are accepted, then the U.S. government could, in theory, impose a *de facto* licensing regime on frontier AI creation and proliferation by suing to enjoin labs from releasing potentially dangerous frontier models publicly.

This, however, would be a novel use of the BWATA and/or the CWCIA. Cases interpreting § 175(a)[194] and § 229[195] have typically dealt with criminal prosecutions for the actual or supposed possession of controlled biological agents or chemical weapons or delivery systems. There is no precedent for a civil suit under §§ 177 or 229D to enjoin the creation or proliferation of a dual-use technology that could be used by a third party to assist in the creation of biological or chemical weapons. Furthermore, it is unclear whether courts would accept that the creation of such a dual-use model rises to the level of "knowingly" assisting in the development of chemical or biological weapons or preparing to knowingly assist in the development of chemical weapons.[196]

A further obstacle to the effective use of the BWATA and/or CWCIA for oversight of AI creation or proliferation is the lack of any existing regulatory apparatus for oversight. BIS oversees a licensing regime implementing certain provisions of the Chemical Weapons Convention,[197] but this regime restricts only the actual production or importation of restricted chemicals, and says nothing about the provision of tools that could be used by third parties to produce chemical weapons.[198] To effectively implement a systematic licensing regime based on §§ 177 and/or 229D, rather than an ad hoc series of lawsuits attempting to restrict specific models on a case-by-case basis, new regulations would need to be promulgated.

---

[191] Convention on the Prohibition of the Development, Production, Stockpiling, and Use of Chemical Weapons and on Their Destruction. S. Treaty Doc. No. 103–21, 1974 U.N.T.S. 317.
[192] 18 U.S.C. § 229.
[193] 18 U.S.C. § 229D.
[194] See, e.g., *United States v. Le*, 902 F.3d 104 (2d Cir. 2018) (affirming conviction under 18 U.S.C. § 175(a) for defendant who unsuccessfully attempted to buy ricin from an undercover FBI agent). But courts have interpreted "biological agent" and "use as a weapon" somewhat broadly. See *United States v. Perez*, 43 F.4th 437, 443 (5th Cir. 2022) (affirming a defendant's conviction under 18 U.S.C. § 1038(a)(1), which criminalizes hoax violations of § 175, for a hoax in which the defendant threatened to pay a person infected with COVID to lick items in two Texas grocery stores.).
[195] See *Bond v. United States*, 572 U.S. 844 (2014) (adopting a narrow reading of § 229 and holding that, under federalism principles, the use of chemicals for an "unremarkable local offense" of "an amateur attempt by a jilted wife to injure her husband's lover, which ended up causing only a minor thumb burn" was not a violation of § 229, which concerns "acts of war, assassination, and terrorism").
[196] See, e.g., *Atchley v. AstraZeneca UK Ltd.*, 22 F.4th 204, 220–24 (D.C. Cir. 2022) (discussing requirements for finding aiding-and-abetting liability in civil and criminal contexts, including the requirements that "defendant must be generally aware of his role as part of an overall illegal or tortious activity at the time that he provides the assistance" and that "defendant must knowingly and substantially assist the principal violation," in case about medical supply companies alleged to have financially supported terrorist organization).
[197] See 15 C.F.R. §§ 710–721.
[198] See 15 C.F.R. §§ 712.2, 713.1.

Federal Select Agent Program

→ Potentially applicable to: Tracking and/or Licensing AI Creation and Proliferation
→ Unlikely to be used for AI Oversight

Following the anthrax letter attacks that killed 5 people and caused 17 others to fall ill in the fall of 2001, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 ("BPRA")[199] in order "to improve the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies."[200] The BPRA authorizes HHS and the United States Department of Agriculture to regulate the possession, use, and transfer of certain dangerous biological agents and toxins; this program is known as the Federal Select Agent Program ("FSAP").

The BPRA includes, at 42 U.S.C. § 262a, a section that authorizes "Enhanced control of dangerous biological agents and toxins" by HHS. Under § 262a(b), HHS is required to "provide for… the establishment and enforcement of safeguard and security measures to prevent access to [FSAP agents and toxins] for use in domestic or international terrorism or for any other criminal purpose."[201]

Subsection 262a(b) is subtitled "Regulation of transfers of listed agents and toxins," and existing HHS regulations promulgated pursuant to § 262a(b) are limited to setting the processes for HHS authorization of transfers of restricted biological agents or toxins from one entity to another.[202] However, it has been suggested that § 262a(b)'s broad language could be used to authorize a much broader range of prophylactic security measures to prevent criminals and/or terrorist organizations from obtaining controlled biological agents. A recent article in the Journal of Emerging Technologies argues that HHS has statutory authority under § 262a(b) to implement a genetic sequence screening requirement for commercial gene synthesis providers, requiring companies that synthesize DNA to check customer orders against a database of known dangerous pathogens to ensure that they are "not unwittingly participating in bioweapon development."[203]

As discussed in the previous section, one of the primary risks posed by frontier AI models is that sufficiently capable models will facilitate the synthesis by criminal or terrorist organizations of dangerous biological agents, including those agents regulated under the FSAP. HHS's Office for the Assistant Secretary of Preparedness and Response also seems to view itself as having authority under the FSAP to make regulations to protect against synthetic "novel high-risk pathogens."[204] If HHS decided to adopt an extremely broad interpretation of its authority under § 262a(b), therefore, it could in theory "establish[] and enforce[]... safeguard and security measures to prevent access" to agents and toxins regulated by the FSAP by creating a system for Oversight of frontier AI models. HHS is not well-positioned, either in terms of resources or technical expertise, to regulate frontier AI models generally, but might be capable of effectively overseeing a

[199] Pub. L. No. 107-188, 116 Stat. 594.
[200] H.R. Rep. No. 107-481, at 1 (2002) (Conf. Rep.).
[201] 42 U.S.C. § 262a(b)(2).
[202] See 42 C.F.R. § 73.16.
[203] See Braden R. Leach, "The Code of Life and Death," 4 J. Emerging Tech. 44, 63–69 (2023) (offering textualist and legislative history arguments for a broad reading of the language of § 262a to allow HHS wide discretion and a variety of means to establish and enforce security measures to carry out its security and safeguarding duties).
[204] Office of the Secretary, Assistant Secretary for Preparedness and Response (ASPR), "Screening Framework Guidance for Providers and Users of Synthetic Oligonucleotides," 87 Fed. Reg. 25495–499 (Published April 29, 2022)

tracking or licensing regime for AI Creation and Proliferation that covered advanced models designed for drug discovery, gene editing, and similar tasks.[205]

However, HHS appears to view its authority under § 262a far too narrowly to undertake any substantial AI Oversight responsibility under its FPAS authorities.[206] Even if HHS did make the attempt, courts would likely view an attempt to institute a licensing regime solely on the basis of § 262a(b), without any further authorization from Congress, as *ultra vires*.[207] In short, the Federal Select Agent Program in its current form is unlikely to be used for AI Oversight.

[205] See, e.g., Siwei Li *et al.*, "Automated high-throughput genome editing platform with an AI learning in situ prediction model," Nature Communications 13, 7386 (2022).
[206] See Leach, "The Code of Life and Death," at 66 (discussing scope of HHS's current interpretation of § 262a).
[207] Ibid., at 76.

INSTITUTE
FOR LAW & AI

law-ai.org