



TAKING FURTHER AGENCY ACTION ON AI

The White House

By Reed Shaw, Will Dobbs-Allsopp, Anna Rodriguez, Adam Conner, Nicole Alvarez, and Ben Olinsky

Authors' note: For this report, the authors use the definition of artificial intelligence (AI) from the 2020 National Defense Authorization Act, which established the National Artificial Intelligence Initiative.¹ This definition was also used by the 2023 “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.”² Similarly, this report makes repeated reference to “Appendix I: Purposes for Which AI is Presumed to be Safety-Impacting and Rights-Impacting” of the 2024 OMB M-24-10 memo, “Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.”³

[Read the fact sheet](#)

The accompanying fact sheet lists all of the recommendations detailed in this chapter of the report.

The Executive Office of the President (the White House), including its subordinate agencies, can use existing regulations and executive actions—including the administration of federal grants and federal contracts, the Defense Production Act, and the use of emergency powers such as the International Emergency Economic Powers Act (IEEPA)—to potentially address the challenges and opportunities of artificial intelligence (AI). Governing for Impact (GFI) and the Center for American Progress have extensively researched these existing authorities in consultation with numerous subject matter experts. However, the goal is to provoke a generative discussion about the following proposals, rather than outline a definitive executive action agenda. Each potential recommendation will require further vetting before agencies act. Even if additional AI legislation is needed, this menu of potential recommendations to address AI demonstrates that there are more options for agencies to explore beyond their current work and that they cannot and should not wait to utilize existing authorities to address AI.

The White House contains numerous agencies and offices that address issues that intersect with AI, including the Office of Science and Technology Policy (OSTP), the National Economic Council (NEC), the National Security Council, and the Office of the National Cyber Director, among many others. Among the most critical is the Office of Management and Budget (OMB), which is responsible for implementing the president’s policies and contains the Office of Information and Regulatory Affairs (OIRA), the government’s regulatory review apparatus.

The White House has already taken action on AI, including the 2022 White House “Blueprint for an AI Bill of Rights”;⁴ the October 2023 “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”;⁵ new OMB AI guidance for federal agencies finalized in March 2024 on “Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence” (OMB M-24-10 AI guidance);⁶ and the agency inventories and AI use cases⁷ required by the Advancing American AI Act.⁸ Much of the AI work produced by the White House has focused on broad principles, targeted efforts by agencies, and guiding the federal government’s use of AI.

The Office of Management and Budget

As the entity responsible for implementing the president’s agenda across the executive branch,⁹ the OMB will play a critical role in coordinating federal agencies as they work to mitigate the known risks posed by AI. This section explains how the OMB and the president can continue to protect Americans from the known risks of AI, including by issuing new guidance for agencies in their disbursement of federal funds and through an updated regulatory review process.

AI risks and opportunities

Government spending constituted more than a quarter of the nation’s gross domestic product in 2022.¹⁰ It is essential that such spending does not operate at cross purposes with the government’s efforts to mitigate the risks associated with AI. The government should avoid inadvertently or intentionally providing federal money to projects that could supercharge the negative consequences of AI. Relatedly, the government should take steps to ensure that its regulatory efforts—whether they are directly or indirectly related to AI—do not produce unintended consequences that amplify AI risks to the public.

The OMB M-24-10 AI guidance implemented a directive from the executive order on AI to guide “required minimum risk-management practices for Government uses of AI that impact people’s rights or safety.”¹¹ The OMB M-24-10 AI guidance outlined 28 broad purposes where the federal government’s use of AI are “presumed to be safety-impacting” or “rights-impacting.”¹² The Biden administration has identified these categories as those that should be subject to heightened scrutiny and required minimum practices.

Of course, as the OMB recognized in its draft AI guidance for federal agencies, responsibly implemented AI has immense potential to improve operations across the federal government.¹³ For example, AI could assist citizens and businesses in navigating everyday interactions with federal agencies.¹⁴ Additionally, as the October 2023 executive order notes, AI could help identify and remediate

cybersecurity vulnerabilities or aid in health care research and development.¹⁵ The OMB’s approach can appropriately balance the need to mitigate the risks of AI use with the potentially immense upsides.

Current state

The OMB has already incorporated AI risk mitigation into the government’s daily operations.¹⁶ In 2020, OMB issued “Circular M-21-06,” which directed agencies to, among other things, describe the statutes that direct or authorize the agency to issue regulations related to the development or use of AI.¹⁷ However, with the notable exception of the Department of Health and Human Services (HHS),¹⁸ agencies generally failed to comply with this directive.¹⁹

Most recently, following President Joe Biden’s issuance of the October 2023 executive order on AI, the OMB released new draft AI guidance for federal agencies²⁰ and finalized that guidance in March 2024 as the OMB M-24-10 AI guidance.²¹ This AI guidance established new requirements for agencies’ use of AI tools, including “specific minimum risk management practices for uses of AI that impact the rights and safety of the public.”²² These proposed management practices include but are not limited to: completing an AI impact assessment (including the provenance and quality of data used in the AI); testing the AI for performance in a real-world context; independent evaluation; ongoing monitoring and periodic human review; ensuring human decision making is kept in the loop; plain-language documentation; reducing algorithmic bias and using representative data; consulting affected groups; and maintaining opt-out options where practicable.²³ Importantly, this guidance focused primarily on agencies’ procurement and use of AI, and not on their regulatory actions to mitigate AI risks created by private actors,²⁴ although CAP and other groups²⁵ have urged the OMB to redouble its efforts to collect agencies’ inventory of statutory authorities that could apply to AI, as required by Executive Order 13859.²⁶

Relevant statutory authorities

The OMB should consider using its statutory authority regarding federal awards, regulatory review, and federal contracting to address key AI issues within its jurisdiction and to direct the federal government’s AI efforts.

Uniform guidance for federal awards

As part of its mission to harmonize and improve operations across agencies, the OMB has the authority to issue guidance to federal agencies on how to disburse awards of federal financial assistance.²⁷

At 31 U.S.C. § 6307, the U.S. Code authorizes the OMB to “issue supplementary interpretative guidelines to promote consistent and efficient use of procurement contracts, grant agreements, and cooperative agreements.”²⁸ At 31 U.S.C. § 503(a) (2), the OMB is directed to “establish governmentwide financial management policies for executive agencies” and “[p]rovide overall direction and leadership to the executive branch on financial management matters by establishing financial management policies and requirements, and by monitoring the establishment and operation of Federal Government financial management systems.”²⁹

Under this authority, the OMB issued the “Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards,” or uniform guidance, in 2014, which is codified at 2 C.F.R. Part 200. The uniform guidance sets forth procedural and substantive guidelines that federal agencies must follow and may consider when disbursing federal awards to nonfederal entities.³⁰ Among other things, the uniform guidance requires federal agencies to publish a notice of funding opportunity for each award, establish a merit review process for applications, and consider the risks associated with making an award, taking into account the awardee’s financial stability, management controls and methods, and history of performance.³¹ Importantly, federal agencies may make exceptions to the uniform guidance’s requirements in their grant processes, and must do so when required by the federal statute governing a particular award.³²

In addition to the uniform guidance, the OMB often issues guidance in the form of memoranda and circulars to agencies, advising them on how they should disburse federal financial assistance. For example, the OMB issued a 2020 memorandum to agency heads detailing how they could change and relax administrative requirements for grant recipients during the COVID-19 public health emergency.³³ Additionally, in 2023, it released another memorandum applying the “Buy America” provisions from a 2021 executive order and the Infrastructure Investment and Jobs Act to federal grant awardees and subawardees.³⁴

Recommendations

Based on the above-cited authority, the OMB could consider the following actions:

- **Develop guidance that adapts the recent OMB M-24-10 AI guidance³⁵ to apply to AI use by other recipients of federal funds, including grants, loans, and other forms of financial assistance.** The guidance could establish a similar framework for agencies to assess the safety- and rights-impacting purposes of AI from the OMB M-24-10 AI guidance³⁶ and mitigate the harmful consequences of the applicable risks thereof, using minimum practices for AI risk management. The guidance could urge agencies to impose conditions on federal funds to the extent the statutory sources of those funds allow such conditions.

- **Update the uniform guidance for federal awards at 2 C.F.R. Part 200, pursuant to 31 U.S.C. §§ 6307 and 503(a)(2), to incorporate AI risk assessment** – and the steps that applicants are taking to mitigate risks – into agencies’ consideration of applications for federal funding, as permitted by the statutory sources for such funding. Specifically, the OMB could update 2 C.F.R. § 200.206(b)(2) to include an assessment of AI risk within its risk evaluation requirements; update 2 C.F.R. § 200.204(c) to require or suggest that the full text of funding opportunity announcements include any AI risk evaluation requirements; and update 2 C.F.R. § 200.211 to require or recommend that federal award publications include the results of AI risk analyses produced during the application process. The current risk evaluation section permits a federal agency to consider the “applicant’s ability to effectively implement statutory, regulatory, or other requirements imposed on non-Federal entities.”³⁷ A revised uniform guidance could explicitly suggest that federal agencies consider the potential for grantees’ use of AI to impact their ability to comply with such requirements and the impact AI use could have on the other categories of risk specified in the current guidance.

These proposals could help prevent federal funds from going toward projects that might accelerate the proliferation of AI harms that affect the safety of the public or the rights of individuals. Further study is needed to determine the exact form that AI risk analysis in federal awards should take.

Updates to regulatory review

Presidents since Richard Nixon have implemented systematic reviews of rulemakings to ensure consistency with statutes and presidential priorities.³⁸ President Ronald Reagan’s Executive Order 12291 centralized regulatory review in the OIRA, a suboffice of OMB, and required that agencies conduct detailed benefit-cost analyses of proposed regulatory actions.³⁹ And President Bill Clinton’s Executive Order 12866 reduced the scope of regulatory review to only those regulatory actions deemed “significant.”⁴⁰

President Biden most recently revised Executive Order 12866 in April 2023.⁴¹ Among other changes, the revision increased the threshold for “significance,” directed federal agencies to engage underrepresented communities during rulemaking processes, and directed the OMB to make corresponding changes to Circular A-4, which implements the regulatory review process.⁴²

AI has the potential to impact every aspect of our economy, government, and society—as evidenced by the expansive scope of the October 2023 executive order on AI,⁴³ the myriad safety-impacting and rights-impacting government uses of AI in the OMB M-24-10 AI guidance,⁴⁴ and the wide range of topics contemplated

in the 2023 OSTP request for information for a national AI strategy.⁴⁵ It is thus reasonable that all regulatory agencies should start to consider the impact of AI on their existing and future abilities to carry out their regulatory requirements.

Recommendations

Based on the above-cited authority, the president, OMB, and OIRA could consider the following actions:

- **Issue a new requirement in the regulatory review process that would require agencies to include a brief assessment of 1) the potential effects of significant regulatory actions on AI development, risks, harms, and benefits, and 2) an assessment of the current and anticipated use of AI by regulated entities and how that use is likely to affect the ability of any proposed or final rule to meet its stated objectives.** This requirement could follow the format of the benefit-cost analysis required by the current Executive Order 12866. The modification to the regulatory review process could take the form of a new executive order, a presidential memorandum,⁴⁶ or an amendment to Executive Order 12866 that adds a subsection to §1(b) and/or §6(a).

- **Issue a presidential memorandum directing agencies and encouraging independent agencies to review their existing statutory authorities to address known AI risks** and consider whether addressing AI use by regulated entities through new or ongoing rulemakings would help ensure that this use does not undermine core regulatory or statutory goals. Such a presidential memorandum would primarily give general direction, similar to the Obama administration's behavioral sciences action,⁴⁷ rather than require a specific analysis on every regulation.

The presidential memorandum could direct executive departments and agencies, or perhaps even the chief AI officer established in the 2023 executive order on AI and further detailed in the OMB M-24-10 AI guidance,⁴⁸ to:

- Identify whether their policies, programs, or operations could be undermined or impaired by the private sector use of AI tools.
- Comprehensively complete the inventory of statutory authorities first requested in OMB Circular M-21-06,⁴⁹ which directed agencies to evaluate their existing authorities to regulate AI applications in the private sector.
- Outline strategies for deploying such statutory authorities to achieve agency goals in the face of identified private sector AI applications.

Federal contracting

Among its recent AI initiatives, the Biden administration has taken steps to address AI in federal contracting. The October 2023 executive order on AI encouraged the U.S. Department of Labor (DOL) to develop nonbinding nondiscrimination guidance for federal contractors using AI in their hiring processes,⁵⁰ which the DOL issued in April 2024.⁵¹ Additionally, the OMB M-24-10 AI guidance both offers and anticipates additional guidance concerning a distinct issue: agencies' procurement of AI tools.⁵²

This section proposes more forceful action. Through the Federal Property and Administrative Services Act (FPASA),⁵³ the federal government retains the authority to impose binding conditions that promote economy and efficiency in federal procurement⁵⁴ on federal contractors,⁵⁵ who collectively employ 1 in 5 U.S. workers.⁵⁶ This section explains why and how the administration could issue binding regulations to protect the federal contracting workforce from nefarious or poorly developed AI management tools, including but not limited to preventing discrimination in hiring. It also explains why the logic underpinning recent adverse FPASA court decisions would not apply to FPASA conditions on using AI management tools.

AI risks and opportunities

AI harms in the workplace are well documented,⁵⁷ and government contractors are not immune to these common problems. Many of these harms are explored in more depth in Chapter V, which discusses AI harms affecting all workers. These include discrimination, safety and health, wage and hour compliance, misclassification of employee roles, worker power and datafication, and workforce training and displacement.⁵⁸ In the federal contracting context, several harms present unique challenges:

- **Discrimination:** For example, as highlighted in the AI Bill of Rights, automated workplace algorithms, which often rely on AI models, have been shown to produce biases in hiring, retention, and firing processes.⁵⁹ The OMB M-24-10 AI guidance highlighted that government use of AI to “[d]etermin[e] the terms or conditions of employment, including pre-employment screening, reasonable accommodation, pay or promotion, performance management, hiring or termination,” should be presumed rights-impacting.⁶⁰ For example, a now-discontinued hiring tool built and used by Amazon was reported to reject women applicants by penalizing resumes that included the word “women’s” in their candidate ranking.⁶¹
- **Physical and mental health harms:** Automated management increases worker physical and mental health risks⁶² and has dire implications for employee privacy.⁶³ The OMB M-24-10 AI guidance highlighted that government use of AI

to incorporate “time-on-task tracking; or conducting workplace surveillance or automated personnel management” should be presumed rights-impacting.⁶⁴

- **Privacy breaches:** Of particular importance to government contracting, AI technologies may increase government vulnerability to privacy breaches when contractors are tasked with handling sensitive data or tasks.⁶⁵
- **Wage and hour compliance:** As technology blurs the line between work and nonwork time, it may become more difficult to assess what time is compensable and therefore should be considered in producing pay determinations. Other risks include opacity and manipulation in algorithmic wage-setting technologies⁶⁶ and digital wage theft enabled by timesheet rounding.⁶⁷

Of course, AI offers opportunities to promote the interests of the federal contracting workforce as well. For example, AI tools could potentially allow compliance officers to better identify violations of preexisting FPASA standards.

Current state

The executive order on AI required the DOL to issue guidance for federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems.⁶⁸ The DOL has recently finalized that guidance.⁶⁹ The guidance explains how federal contractors and subcontractors who use AI, algorithms, and automated systems may be at risk of violating the Equal Employment Opportunity Act and provides examples of how contractors can meet their compliance obligations.⁷⁰ Importantly, the guidance states that federal contractors cannot delegate compliance responsibilities to outside entities, including vendors, and provides several promising practices to maintain compliance.⁷¹

Separately, the OMB M-24-10 AI guidance has proposed standards for agencies’ procurement of AI technology and promises to “develop an initial means to ensure that Federal contracts for the acquisition of an AI system or service align with the guidance in this memorandum”⁷² in accordance with the Advancing American AI Act,⁷³ which was signed into law in December 2022,⁷⁴ and the 2023 executive order on AI.⁷⁵ On March 29, 2023, the OMB posted a request for information on “Responsible Procurement of Artificial Intelligence in Government” to help develop that guidance.⁷⁶

Despite these important steps, neither the executive order on AI, the OMB M-24-10 AI guidance, nor future AI procurement guidance announced in the OMB M-24-10 AI guidance appears likely to cover the AI tools federal contractors may be using to manage their workforces outside of hiring.

Relevant statutory authority

The FPASA authorizes the president to “prescribe policies and directives that the President considers necessary to carry out this subtitle,” namely the FPASA’s goal of promoting economy or efficiency in federal procurement.⁷⁷

Past administrations have invoked the FPASA to regulate federal contracting in various ways. In the 1970s, courts held that the FPASA authorized the federal government to require contractors to abide by certain anti-discrimination policies.⁷⁸ Other administrations have invoked the FPASA to require federal contractors to comply with certain workplace standards, including wage and price standards,⁷⁹ regulations concerning project labor agreements,⁸⁰ and requirements that contractors provide employees notice of their rights to opt out of joining a union or paying mandatory dues outside of representational activities.⁸¹ The federal government has also promulgated FPASA rules requiring contractors to provide disclosures of known violations of federal criminal laws or of the civil False Claims Act,⁸² creating business ethics awareness and compliance programs,⁸³ and mandating the use of the E-Verify system to confirm employment eligibility of workers.⁸⁴ In 2011, the Obama administration used the FPASA to mandate that contractors implement screening systems to prevent employee conflicts of interest.⁸⁵ And in 2016, the Obama administration relied on its FPASA authority to require federal contractors to receive paid sick leave.⁸⁶

More recently, the Biden administration has deployed its FPASA authority in two high-profile cases: 1) to impose a vaccine or test mandate on the federal contracting workforce and 2) to raise the minimum wage for federal contractors’ employees to \$15 per hour in 2022.⁸⁷ Challengers have successfully won injunctions against both rules in federal courts—although, as explained below, for reasons that do not apply to this proposal.⁸⁸

Recommendations

As the OMB prepares the forthcoming procurement guidance mentioned in OMB M-24-10 AI guidance,⁸⁹ it may also want to consider whether it can include standards that:

- **Ensure baseline levels of competition and interoperability**, such that agencies do not get locked into using the services of a single AI firm.

Under its FPASA authority, the Federal Acquisition Regulatory Council,⁹⁰ which is chaired by OMB’s administrator for federal procurement policy, can promulgate a rule that outlines protections for all employees at firms that hold a federal contract as it relates to AI, including potentially through the following actions:

- **Incorporate the presumed safety-impacting and rights-impacting uses of AI** from the OMB M-24-10 AI guidance to apply to federal contractors and their use of AI systems for workplace management.⁹¹
- **Require federal contractors employing automated systems to use predeployment testing and ongoing monitoring** to ensure safety and that workers are paid for all compensable time and to mitigate other harmful impacts.
- **Establish specific requirements regarding pace of work, quotas, and worker input** to reduce the safety and health impacts of electronic surveillance and automated management.
- **Mandate disclosure requirements** when employees are subject to automation or other AI tools.
- **Provide discrimination protections** related to algorithmic tools, including ensuring that automated management tools can be adjusted to make reasonable accommodations for workers with disabilities.
- **Ensure privacy protections** for employees and users of AI.

Many of these recommendations follow from the executive order on AI,⁹² the OMB M-24-10 AI guidance,⁹³ the AI Bill of Rights,⁹⁴ and the National Institute of Standards and Technology (NIST) AI Risk Management Framework;⁹⁵ other standards from these documents may also be worth considering.

Regulating the use of AI in government contracts advances the FPASA’s statutory goals of economy and efficiency in several ways. For example, AI hiring tools often rely on data that already suffers from bias,⁹⁶ and relying on AI tools may bake in this data and mask it from potential employers. These biases may increase employee turnover and make contractors vulnerable to legal risks, leading to increased costs for contractors and the government. Furthermore, AI models such as algorithmic management have been linked to safety issues, including increased stress for workers under employer surveillance.⁹⁷ Worker stress can lead to increased mistakes and safety issues, creating added costs for the government down the line.

These justifications find close analogs in the reasoning that past administrations have used to impose new FPASA obligations that have been upheld in federal court. For example, in *Chamber of Commerce v. Napolitano*, a federal district court upheld a requirement that contractors ascertain the immigration status of certain new hires using E-Verify, finding that a reasonably close nexus exists so long as the “President’s explanation for how an Executive Order promotes efficiency

and economy [is] reasonable and rational.”⁹⁸ In that case, the court found that President George W. Bush’s conclusion that the E-Verify system would result in fewer immigration enforcement actions, fewer undocumented workers—and “therefore generally more efficient and dependable procurement sources”—was sufficient to meet the nexus requirement.⁹⁹ The court also held that “[t]here is no requirement ... for the President to base his findings on evidence included in a record.”¹⁰⁰ Similarly, in this context, regulating the use of AI in government contracts would also lead to a more “dependable procurement” workforce since AI technologies would be tested to root out possible bias or other automation harms. Additionally, some of the earliest exercises of modern presidential procurement power concerned anti-discrimination measures.¹⁰¹

Finally, it is important to note that two high-profile efforts by the Biden administration to impose laudable requirements on federal contractors have suffered setbacks in court. One was an order,¹⁰² enjoined by the 5th, 6th, and 11th U.S. Circuit Courts of Appeals,¹⁰³ obligating contract recipients to require their employees to wear face masks at work and be vaccinated against COVID-19. Another order increased the hourly minimum wage paid by parties who contract with the federal government for workers on or in connection with a federal government contract.¹⁰⁴ Despite favorable district court rulings in Arizona and Colorado,¹⁰⁵ a court in the Southern District of Texas enjoined the application of the minimum wage rule in three Southern states.¹⁰⁶ Recently, however, the 10th U.S. Circuit Court of Appeals upheld the minimum wage rule as applied to seasonal recreational workers, finding that the standard for finding a nexus between the rule and FPASA’s goal of “economy and efficiency” is lenient.¹⁰⁷

However, this proposed rule is distinguishable from the minimum wage and COVID-19 rules in several ways. In the COVID-19 case, the 5th Circuit, citing the major questions doctrine, found the FPASA did not clearly authorize the president to impose requirements concerning the conduct of the employees of federal contractors, as opposed to regulating the contractor-employers themselves.¹⁰⁸ A rule regulating the use of AI in government contracts would not impose any requirements on employee conduct, even indirectly. Hence, this decision is largely irrelevant to the proposed action.

Even according to the flawed reasoning of the Texas district court’s opinion enjoining the minimum wage rule in three states, the administration could distinguish a rule regulating the use of AI under several theories. For one, regulating the use of AI would not have nearly the same economic ramifications for contractors since it would not require immediate wage increases across the workforce. The proposed rule’s focus would be quality assurance for the use of AI systems, leading to likely savings for the government—the kind of purchasing considerations that fit squarely within the court’s framing of the FPASA as primarily concerned with the “supervisory role of buying and selling of goods.”¹⁰⁹

Defense Production Act

The Defense Production Act (DPA) includes a powerful and underutilized subpoena power that may offer the best opportunity for the federal government to get a look inside certain AI models.¹¹⁰

Current state

The executive order on AI laudably invokes the DPA to impose a limited disclosure obligation on the developers of certain new AI models.¹¹¹ Specifically, the executive order directs the U.S. Department of Commerce to require companies “developing or demonstrating an intent to develop potential dual-use foundation models” to report—on an ongoing basis—training parameters, model weights, and “red-teaming” testing results based on forthcoming NIST guidance.¹¹² According to a news report, these requirements will apply to “all future commercial AI models in the US, but not apply to AI models that have already been launched.”¹¹³ The executive order also directs the Department of Commerce to require that people or companies that acquire, develop, or possess “a potential large-scale computing cluster” report the existence and location of those clusters.¹¹⁴

Relevant statutory authority

The executive order’s disclosure directive is well-grounded in statutory authority, as illustrated below. This section seeks to underscore that the president’s DPA authority plausibly extends beyond what the proposal laid out in the executive order.

When it comes to subpoenas, the DPA holds:

*The president shall be entitled ... to obtain such information from, require such reports and the keeping of such records by, make such inspection of the books, records, and other writings, premises or property of ... any person as may be necessary or appropriate, in [the President’s] discretion, to the enforcement or the administration of this chapter and the regulations or orders issued thereunder ... [and] to obtain information in order to perform industry studies assessing the capabilities of the United States industrial base to support the national defense.*¹¹⁵

This language is quite broad, particularly in the first grant of authority. The second, more qualified grant for industry studies, at least references the terms “industrial base,” which is not defined in the statute, and “national defense,” which is statutorily defined in part as “critical infrastructure protection and restoration.”¹¹⁶ “Critical infrastructure” is defined, in turn, as “any systems and assets, whether physical or cyber-based, so vital to the United States that the degradation or destruction of such systems and assets would have a debilitating

impact on national security, including, but not limited to, national economic security and national public health or safety.”¹¹⁷ There exists a presumption, waivable by the president, of confidentiality if the company so attests, per 50 U.S.C. §4555(d).¹¹⁸

Beyond military applications, then, the DPA’s subpoena power appears to extend, at minimum, to any AI application that poses a serious threat to basic services—for example, the energy grid or water system—the broader economy, or public health. Notably, the executive order’s definition of dual-use foundation models appears to be somewhat coextensive with the DPA’s definition of “critical infrastructure.”¹¹⁹

However, it is worth emphasizing that the DPA empowers the president to take additional action if necessary. For example, nothing in the statute prevents the administration from applying its reporting requirements to existing AI applications, rather than future ones, as reporting indicates is the current plan.¹²⁰ Indeed, while the executive order envisions creating an ongoing notification and reporting system, the president still retains the statutory authority to demand, on a one-off basis, a broad array of information from companies that own AI applications capable of threatening the statute’s capacious definition of “national defense.” This authority similarly would allow the president to seek relevant information beyond training parameters, model weights, and red-teaming test results.

Emergency powers

As the nation’s chief executive, the president has a constitutional obligation to respond to exigent national security threats and national emergencies.¹²¹ Additionally, Congress has enacted specific statutory schemes endowing the president with enhanced powers under certain emergent circumstances.¹²² This section explains several potential applications of the president’s emergency powers that are relevant to known risks of AI. It suggests that the White House define the criteria that would lead the president to use these authorities. It also proposes drafting an emergency response plan the government can follow once those criteria are met.

AI risks and opportunities

It is possible that some future AI application may suddenly pose risks that demand an exigent response. Examples of such circumstances might include:

- **Financial chaos:** AI used in stock prediction and financial decision-making may raise the risk of stock market collapse by increasing the homogeneity of stock trading. As Securities and Exchange Commission (SEC) Chair Gary Gensler warned in a 2020 paper, if trading algorithms all make a simultaneous decision to

sell the same asset, it could tank the stock market.¹²³ Sens. Mark Warner (D-VA) and John Kennedy (R-LA) have introduced legislation to address threats to financial markets from AI, with Sen. Warner noting, “AI has tremendous potential but also enormous disruptive power across a variety of fields and industries – perhaps none more so than our financial markets.”¹²⁴

- **National security and biodefense:** Some of the same features that make AI revolutionary technology with great potential for good—for instance, reducing cost and complexity of scientific endeavors—may also pose national security threats. AI may make it easier for foreign governments and nonstate actors to achieve breakthroughs in areas such as autonomous weaponry, biological warfare, and mass manipulation through high-quality mis-/dis-/mal-information. Any or all the above could threaten the nation’s security.¹²⁵ The 2023 executive order on AI outlined numerous taskings related to addressing AI’s impact on cybersecurity and biosecurity.¹²⁶
- **Corrupted information and weaponized communications:** The 2022 National Science and Technology Council (NSTC) report, “Roadmap for Researchers on Priorities Related to Information Integrity Research and Development,” noted four main categories of harms from corrupted information: harms to consumers and companies, individuals and families, national security, and society and the democratic process.¹²⁷ In particular, experts repeatedly cite rapidly disseminated and weaponized information campaigns as a key threat of greatly expanded AI. AI allows bad actors to create and publish enormous amounts of mis-/dis-/mal-information that are difficult to distinguish from truth.¹²⁸ Increasingly sophisticated AI will exploit “cognitive fluency bias,” which refers to humans’ tendency to give more weight to information conveyed in well-written text content or compelling visuals.¹²⁹ This kind of misinformation is already a key strategy of nonstate and state actors in Russia, China, and Iran, among other countries.¹³⁰ For instance, a crude version of this “deepfake” strategy was deployed in the Russian war against Ukraine, wherein the Russian government published an AI-generated video of Ukrainian President Volodymyr Zelenskyy calling on Ukrainians to lay down their arms.¹³¹ In May 2024, before the U.S. Senate Select Committee on Intelligence, Director of National Intelligence Avril Haines testified:

For example, innovations in AI have enabled foreign influence actors to produce seemingly-authentic and tailored messaging more efficiently, at greater scale, and with content adapted for different languages and cultures. In fact, we have already seen generative AI being used in the context of foreign elections.¹³²

Current state

The national security apparatus has begun to react to the potential threats of AI proliferation. Officials at the U.S. Department of Defense have taken steps to better defend the country's information ecosystem from rapidly proliferating dis-/mis-/mal-information,¹³³ issued the 2022 “Responsible Artificial Intelligence Strategy and Implementation Pathway” report,¹³⁴ and spoken publicly about the U.S. military's AI strategy.¹³⁵

In August 2023, President Biden signed Executive Order 14105, “Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern.”¹³⁶ This executive order declared a national emergency based on advances made by “countries of concern” in “sensitive technologies and products critical for the military, intelligence, [and] surveillance.”¹³⁷ The president issued the executive order pursuant to the International Emergency Economic Powers Act (IEEPA). The executive order included AI in its list of sensitive technologies and directed the U.S. Treasury Department to prohibit outbound investments into those countries of concern and to establish strict regulatory requirements in other countries.¹³⁸ Relatedly, the Commerce Department initiated export controls in October 2022 that restrict the ability of companies to sell certain advanced computing semiconductors or related manufacturing equipment to China.¹³⁹ The Commerce Department expanded its AI export controls in October 2023.¹⁴⁰

The 2023 executive order on AI also recognized the potential national security implications of the spread of AI, and directed agency actions to mitigate AI risks in critical infrastructure and cybersecurity.¹⁴¹ The order highlighted the potential for AI to increase biosecurity risks and directed various stakeholders to produce a study of those risks and potential mitigation options.¹⁴² The executive order also tasked the national security adviser with delivering an additional “National Security Memorandum” on AI to the president in 2024.¹⁴³

As noted above, President Biden declared a national emergency pursuant to the IEEPA in August 2023 with Executive Order 14105,¹⁴⁴ which joined other emergencies involving technology declared via executive order. This includes a national emergency declared in President Donald Trump's May 2019 Executive Order 13873, “Securing the Information and Communications Technology and Services Supply Chain”;¹⁴⁵ it was further expanded by President Biden's June 2021 Executive Order 14034, “Protecting Americans' Sensitive Data From Foreign Adversaries,”¹⁴⁶ and again in his February 2024 Executive Order 14117, “Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.”¹⁴⁷ Executive Order 14117 directed various federal agencies to issue regulations prohibiting data transfers—through data brokers, employment agreements, investment agreements, and otherwise—to “countries of concern.”¹⁴⁸

Relevant authorities

This section identifies ways that the president could exercise their authority in the event of—and in anticipation of—AI systems that may pose a threat to the safety of the American people. Upon the president’s declaration of a national emergency, several authorities throughout the U.S. Code become available.¹⁴⁹ These include economic tools such as the IEEPA,¹⁵⁰ which authorizes the president to regulate or prohibit international transactions in the event of a national emergency. Since the law’s enactment, presidents have declared 69 emergencies pursuant to the IEEPA.¹⁵¹ At 50 U.S.C. § 1701, the IEEPA authorizes the president to use the statute’s authorities “to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat.”¹⁵² Subject to some exceptions,¹⁵³ upon declaration of a national emergency, 50 U.S.C. § 1702 provides the president with authority to take extensive action to “investigate, regulate, or prohibit” a wide range of international transactions and freeze assets of foreign actors.¹⁵⁴ At 50 U.S.C. § 1708(b), the IEEPA authorizes the president to “block and prohibit all transactions in all property and interests in property of” foreign persons or entities engaged in or benefiting from “economic or industrial espionage in cyberspace, of technologies or proprietary information developed by United States persons.”¹⁵⁵

Available emergency authorities also include infrastructural powers such as those the president possesses over the nation’s communications infrastructure. For example, under the Communications Act at 47 U.S.C. § 606(c), upon “proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States,” the president may suspend or amend regulations applicable to any or all stations or devices capable of emitting electromagnetic radiation and may cause the closing of any radio station.¹⁵⁶

The president also possesses emergency powers to modify federal contracts. At 41 U.S.C. § 3304, the U.S. Code authorizes executive agencies to use noncompetitive procurement procedures if “it is necessary to award the contract to a particular source to maintain a facility, producer, manufacturer, or other supplier available for furnishing property or services in case of a national emergency or to achieve industrial mobilization.”¹⁵⁷

In addition to these and more specific statutory authorities, the president also possesses inherent Article II authority to protect the country from immediate threats in other ways.¹⁵⁸ As the U.S. Supreme Court has long recognized, circumstances may arise that demand presidential action in the absence of congressional delegation—particularly, during emergency situations.¹⁵⁹ CAP has

previously highlighted the need for the administration to prepare to address AI systems that may threaten the safety of the American people.¹⁶⁰

Recommendations

To prepare the government to use the above powers in the event of an AI system posing emergency threats to the United States, the White House could consider the following actions:

- **Direct the National Security Council to develop a memorandum that outlines scenarios wherein AI applications could pose an emergency threat to the country and identifies actions that the president could take through existing statutory schemes and their inherent executive authority under Article II of the Constitution to resolve the threat.** The memorandum should study the landscape of imaginable AI applications and devise criteria that would trigger emergency governmental action. Such a memorandum could complement or be incorporated as part of the National Security Memorandum required by the October 2023 executive order on AI.¹⁶¹ The memorandum's design could echo the National Response Plan, originally developed after 9/11 to formalize rapid government response to terrorist attacks and other emergency scenarios.¹⁶² The memorandum could consider authorities:
 - **Inherent to the president's constitutional prerogative to protect the nation:** For example, the memorandum could identify when it could be appropriate for the president to take military or humanitarian action without prior congressional authorization when immediate action is required to prevent imminent loss of life or property damage.¹⁶³
 - **Under the IEEPA:** For example, the memorandum could consider the administration's authority to expand the policies established in the August 2023 IEEPA executive order, using the statute to freeze assets associated with AI technologies and countries of concern that contribute to the crisis at hand.¹⁶⁴ Follow-up executive action could identify new countries of concern as they arise. As another example, the memorandum could identify triggers for pursuing sanctions under 50 U.S.C. § 1708(b) on foreign persons that support the use of proprietary data to train AI systems or who steal proprietary AI source code from sources in the United States. The memorandum could also explore the president's authority to investigate, regulate, or prohibit certain transactions or payments related to run away or dangerous AI models in cases where the models are trained or operate on foreign-made semiconductors and the president determines that such action is necessary to "deal with" a national security threat. Even if that model is deployed domestically or developed by a domestic entity, it may still fall within reach of the IEEPA's potent §1702 authorities if, per 50 U.S.C. §1701, the model: 1) poses an "unusual or extraordinary threat," and 2) "has its source in whole or substantial part outside the United States." The administration can explore whether AI models' dependence on foreign-made semiconductors for training

and continued operation meets this second requirement. Indeed, scholars have previously argued that the interconnectedness of the global economy likely subjects an array of domestic entities to IEEPA in the event sufficiently exigent conditions arise.¹⁶⁵

- **Under the Communications Act:** For example, the memorandum could identify scenarios in which the president could consider suspending or amending regulations under 47 U.S.C. § 606(c) regarding wireless devices to respond to a national security threat.¹⁶⁶ The bounds of this authority are quite broad, covering an enormous number of everyday devices, including smartphones that can emit electromagnetic radiation.¹⁶⁷
 - **To modify federal contracts:** For example, the memorandum could identify possibilities for waiving procurement requirements in a national emergency if quickly making a federal contract with a particular entity would help develop capabilities to combat a rapidly deploying and destructive AI.¹⁶⁸
 - **To take other statutorily or constitutionally authorized actions:** The memorandum could organize a process through which the White House and national security apparatus would, upon the presence of the criteria outlined in the memorandum, assess an emergent AI-related threat, develop a potential response, implement that response, and notify Congress and the public of such a response.¹⁶⁹ It could also request a published opinion from the Office of Legal Counsel on the legality of the various response scenarios and decision-making processes drawn up pursuant to the recommendations above. This will help ensure that the president can act swiftly but responsibly in an AI-related emergency.
- **Share emergency AI plans with the public:** The administration should share such emergency processes and memoranda they develop with Congress, relevant committees, and the public where possible.

Conclusion

The White House and its subordinate agencies, including the OMB and OIRA, have taken important steps to begin safeguarding government operations and the public from the potential harms of AI. Yet as this section illustrates, policymakers nonetheless retain a number of untapped tools at their disposal that should be further considered to address AI. As AI control technologies and protocols cohere in the coming years, GFI and CAP hope that the preceding recommendations empower officials to think broadly about how executive action could help build a safe and productive AI ecosystem.

Read the fact sheet

The accompanying fact sheet lists all of the recommendations detailed in this chapter of the report.

Endnotes

- 1 Office of the Law Revision Counsel, "15 USC 9401(3): Definitions," available at [\(https://uscode.house.gov/view.xhtml?req=\(title:15%20section:9401%20edition:prelim\)\)](https://uscode.house.gov/view.xhtml?req=(title:15%20section:9401%20edition:prelim)) (last accessed May 2024).
- 2 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Federal Register 88 (210) (2023): 75191–75226, available at <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>.
- 3 Shalanda D. Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (Washington: Office of Management and Budget, 2024), available at <https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf>.
- 4 The White House, "Blueprint for an AI Bill of Rights" (Washington: The White House, 2022), available at <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.
- 5 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- 6 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
- 7 AI.gov, "The Government Is Using AI to Better Serve the Public," available at <https://ai.gov/ai-use-cases/> (last accessed February 2024).
- 8 Advancing American AI Act, 40 U.S.C. 11301 (May 13, 2024), available at [\(https://uscode.house.gov/view.xhtml?req=\(title:40%20section:11301%20edition:prelim\)\)](https://uscode.house.gov/view.xhtml?req=(title:40%20section:11301%20edition:prelim)).
- 9 The White House, "Office of Management and Budget," available at <https://www.whitehouse.gov/omb/> (last accessed February 2024).
- 10 U.S. Treasury Fiscal Data, "How much has the U.S. government spent this year?," available at <https://fiscaldata.treasury.gov/americas-finance-guide/federal-spending/> (last accessed February 2024).
- 11 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- 12 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Appendix I pp. 31–33.
- 13 Ibid.
- 14 Niklas Berglind, Ankit Fadia, and Tom Isherwood, "The potential value of AI – and how governments could look to capture it," McKinsey & Company, July 25, 2022, available at <https://www.mckinsey.com/industries/public-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it>.
- 15 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- 16 Russell T. Vought, "M-21-06 Memorandum for the Heads of Executive Departments and Agencies: Guidance for Regulation of Artificial Intelligence Applications" (Washington: Office of Management and Budget, 2020), available at <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf>.
- 17 Ibid.
- 18 U.S. Department of Health and Human Services, "OMB M-21-06 (Guidance for Regulation of Artificial Intelligence Applications)," available at <https://www.hhs.gov/sites/default/files/department-of-health-and-human-services-omb-m-21-06.pdf> (last accessed 2024).
- 19 One analysis found that 88 percent of agencies did not publish an inventory of AI authorities. See Christie Lawrence, Isaac Cui, and Daniel E. Ho, "Implementation Challenges to Three Pillars of America's AI Strategy" (Stanford, CA: Stanford Institute for Human-Centered Artificial Intelligence and Stanford Regulation, Evaluation, and Governance Lab, 2022), available at <https://hai.stanford.edu/sites/default/files/2022-12/HAIRegLab%20White%20Paper%20-%20Implementation%20Challenges%20to%20Three%20Pillars%20of%20America%E2%80%99s%20AI%20Strategy.pdf>; Madison Alder and Rebecca Heilweil, "Ex-White House official says improved artificial intelligence inventories could help OMB guidance," FedScoop, September 29, 2023, available at <https://fedscoop.com/improved-artificial-intelligence-inventories-could-help-guidance/>.
- 20 Shalanda D. Young, "Proposed Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Office of Management and Budget, October 30, 2023, available at <https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf>.
- 21 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
- 22 Ibid., p. 1.
- 23 Ibid.
- 24 Ibid., p. 2. "[T]his memorandum is more narrowly scoped to address a subset of AI risks, as well as governance and innovation issues that are directly tied to agencies' use of AI."
- 25 Adam Conner, "Re: Request for Comments: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum; FR Doc. 2023-24269, 23 Nov. 2023," Center for American Progress, December 5, 2023, available at <https://www.americanprogress.org/wp-content/uploads/sites/2/2023/12/CAP-Draft-OMB-Comments-Final-12.04.2023.pdf>.
- 26 Executive Office of the President, "Executive Order 13859: Maintaining American Leadership in Artificial Intelligence," Federal Register 84 (31) (2019): 3967–3972, available at <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence>.
- 27 Legal Information Institute, "31 U.S.C. § 6307 - Interpretative guidelines and exemptions," available at <https://www.law.cornell.edu/uscode/text/31/6307> (last accessed February 2024).
- 28 Ibid.
- 29 Legal Information Institute, "31 U.S.C. § 503(a)(2) - Functions of Deputy Director for Management," available at <https://www.law.cornell.edu/uscode/text/31/503> (last accessed February 2024).
- 30 Legal Information Institute, "2 CFR 200.100(a)(1) - Purpose," available at <https://www.law.cornell.edu/cfr/text/2/200.100#-:text=%C2%A7%20200.100%20Purpose.%20%28a%29%20Purpose.%20%281%29%20This%20part,to%20non-Federal%20entities%2C%20as%20described%20in%20%C2%A7%20200.101> (last accessed February 2024).
- 31 Legal Information Institute, "2 CFR 200.206 - Federal awarding agency review of risk posed by applicants," available at <https://www.law.cornell.edu/cfr/text/2/200.206> (last accessed February 2024).

- 32 Legal Information Institute, "2 CFR 200.100(a)(1) - Purpose."
- 33 Michael Rigas, "Memorandum to the Heads of Executive Departments and Agencies: Extension of Administrative Relief for Recipients and Applicants of Federal Financial Assistance Directly Impacted by the Novel Coronavirus (COVID-19) due to Loss of Operations" (Washington: Office of Management, 2020), available at <https://www.whitehouse.gov/wp-content/uploads/2020/06/M-20-26.pdf>.
- 34 Shalanda D. Young, "M-24-02 Memorandum for the Heads of Executive Departments and Agencies: Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure" (Washington: Office of Management and Budget, 2023), available at <https://www.whitehouse.gov/wp-content/uploads/2023/10/M-24-02-Buy-America-Implementation-Guidance-Update.pdf>.
- 35 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
- 36 *Ibid.*, Appendix I.
- 37 Legal Information Institute, "2 CFR § 200.206(b)(2) (v) - Federal awarding agency review of risk posed by applicants."
- 38 Steven A. Engel, "Extending Regulatory Review Under Executive Order 12866 to Independent Regulatory Agencies," October 8, 2019, p. 9, available at <https://www.justice.gov/olc/file/1349716/download>.
- 39 Executive Office of the President, "Executive Order 12291: Federal Regulation," Federal Register 46 (33) (1981): 12941-31398, available at <https://www.archives.gov/federal-register/codification/executive-order/12291.html>.
- 40 Executive Office of the President, "Executive Order 12866: Regulatory Planning and Review," Federal Register 58 (190) (1993): 51735-51744, available at <https://www.archives.gov/files/federal-register/executive-orders/pdf/12866.pdf>.
- 41 Executive Office of the President, "Executive Order 14094: Executive Order on Modernizing Regulatory Review," Federal Register 88 (69) (2023): 21879-21881, available at <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/04/06/executive-order-on-modernizing-regulatory-review/>.
- 42 The White House, "Circular No. A-4: Regulatory Analysis," November 9, 2023, available at <https://www.whitehouse.gov/wp-content/uploads/2023/11/Circular-A-4.pdf>.
- 43 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- 44 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
- 45 Office of Science and Technology Policy, "Request for Information: National Priorities for Artificial Intelligence," Regulations.gov, May 26, 2023, available at <https://www.regulations.gov/document/OSTP-TECH-2023-0007-0001>.
- 46 Executive orders and presidential memoranda differ mostly in form, not substance or effect. See John Contrubis, "Executive Orders and Proclamations" (Washington: American Law Division of the Congressional Research Service, 1999), available at <https://sgp.fas.org/crs/misc/95-772.pdf>. See also, Abigail A. Graber, "Executive Orders: An Introduction" (Washington: Congressional Research Service, 2021), p. 20, available at <https://crsreports.congress.gov/product/pdf/R/R46738>; Todd Garvey, "Executive Orders: Issuance, Modification, and Revocation" (Washington: Congressional Research Service, 2014), p. 1-2, available at <https://crsreports.congress.gov/product/pdf/RS/RS20846>.
- 47 Executive Office of the President, "Executive Order 13707: Using Behavioral Science Insights To Better Serve the American People," Federal Register 80 (181) (2015): 56365-56367, available at <https://www.federalregister.gov/documents/2015/09/18/2015-23630/using-behavioral-science-insights-to-better-serve-the-american-people>.
- 48 The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"; Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
- 49 Vought, "M-21-06 Memorandum for the Heads of Executive Departments and Agencies: Guidance for Regulation of Artificial Intelligence Applications." Most agencies either failed to comply with this directive or did so incompletely. Compare HHS' response with the Department of Energy's U.S. Department of Health and Human Services, "OMB M-21-06 (Guidance for Regulation of Artificial Intelligence Applications)"; U.S. Department of Energy, "DOE AI Report to OMB regarding M-21-06" (Washington: 2021), available at <https://www.energy.gov/articles/m-21-06-regulations-artificial-intelligence>.
- 50 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Section 7.3, p. 75213. "(a) Within 365 days of the date of this order, to prevent unlawful discrimination from AI used for hiring, the Secretary of Labor shall publish guidance for Federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems."
- 51 Office of Federal Contract Compliance Programs, "Artificial Intelligence and Equal Employment Opportunity for Federal Contractors," available at <https://www.dol.gov/agencies/ofccp/ai/ai-eeo-guide> (last accessed April 2024).
- 52 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Section 5(d).
- 53 Federal Property and Administrative Services Act, Public Law 152, 81st Cong., 1st sess. (July 1, 1949), available at <https://disposal.gsa.gov/s/act49>.
- 54 Legal Information Institute, "40 U.S.C. 101 - Purpose"; Legal Information Institute, "40 U.S.C. 121(a) - Administrative."
- 55 Legal Information Institute, "40 U.S.C. 101 - Purpose," available at <https://www.law.cornell.edu/uscode/text/40/101> (last accessed May 2024); Legal Information Institute, "40 U.S.C. 121(a) - Administrative," available at <https://www.law.cornell.edu/uscode/text/40/121> (last accessed May 2024).
- 56 Jessica Guynn and others, "Broken promises: Federal contractors made diversity pledges. They didn't keep them," USA Today, April 30, 2023, available at: <https://www.usatoday.com/story/news/investigations/2023/04/28/federal-contractors-diversity-executive-jobs-fail/11705441002/>.
- 57 Tanya Goldman, "What the Blueprint for an AI Bill of Rights Means for Workers," U.S. Department of Labor, October 4, 2022, available at <https://blog.dol.gov/2022/10/04/what-the-blueprint-for-an-ai-bill-of-rights-means-for-workers>; Aurelia Glass, "Unions Give Workers a Voice Over How AI Affects Their Jobs" (Washington: Center for American Progress, 2024), available at <https://www.americanprogress.org/article/unions-give-workers-a-voice-over-how-ai-affects-their-jobs/>.
- 58 Center for Labor and a Just Economy, "Worker Power and Voice in the AI Response" (Cambridge, MA: Harvard Law School, 2024), available at <https://clje.law.harvard.edu/worker-power-and-voice-in-the-ai-response/>.
- 59 Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights: Algorithmic Discrimination Protections" (Washington: The White House, 2022), available at: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/algorithmic-discrimination-protections-2/>. The recent DOL guidance also highlights how "AI has the potential to embed bias and discrimination into a range of employment decision-making processes." See Office of Federal Contract Compliance Programs, "Artificial Intelligence and Equal Employment Opportunity for Federal Contractors."

- 60 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
- 61 Jeffrey Dastin, "Insight - Amazon scraps secret AI recruiting tool that showed bias against women," Reuters, October 10, 2018, available at <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>.
- 62 Matt Scherer, "Warning: Bossware May be Hazardous to Your Health" (Washington: Center for Democracy and Technology, 2021), available at <https://cdt.org/wp-content/uploads/2021/07/2021-07-29-Warning-Bossware-May-Be-Hazardous-To-Your-Health-Final.pdf>.
- 63 Emma Oppenheim, "Worker surveillance poses potential privacy harms," Consumer Financial Protection Bureau, June 20, 2023, available at <https://www.consumerfinance.gov/about-us/blog/worker-surveillance-poses-potential-privacy-harms/>.
- 64 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Section 5.b.ii.G.
- 65 National Conference of State Legislatures, "NCSL Task Force on Artificial Intelligence, Cybersecurity and Privacy," available at <https://www.ncsl.org/in-dc/task-forces/task-force-on-artificial-intelligence-cybersecurity-and-privacy> (last accessed February 2024).
- 66 Veena Dubal, "The House Always Wins: the Algorithmic Gambification of Work," Law and Political Economy Project, January 23, 2023, available at <https://lpeproject.org/blog/the-house-always-wins-the-algorithmic-gambification-of-work/>; Zephyr Teachout, "Surveillance Wages: A Taxonomy," Law and Political Economy Project, November 6, 2023, available at <https://lpeproject.org/blog/surveillance-wages-a-taxonomy/>.
- 67 Elizabeth Chika Tippett, "How Employers Profit from Digital Wage Theft Under the FLSA," American Business Law Journal 55 (2) (2018): 315–401, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3877641.
- 68 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- 69 Office of Federal Contract Compliance Programs, "Artificial Intelligence and Equal Employment Opportunity for Federal Contractors."
- 70 Ibid.
- 71 Ibid.
- 72 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," p. 24.
- 73 The Advancing American AI Act was incorporated into the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023. See James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, H.R. 7776, 116th Cong., 1st sess. (December 23, 2022), available at <https://www.congress.gov/bill/117th-congress/house-bill/7776>.
- 74 The White House, "Statement by the President on H.R. 7776, the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023," Press release, December 23, 2022, available at <https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/23/statement-by-the-president-on-h-r-7776-the-james-m-inofoe-national-defense-authorization-act-for-fiscal-year-2023/>.
- 75 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- 76 Office of Management and Budget, "Request for Information: Responsible Procurement of Artificial Intelligence in Government" Federal Register 89 (62) (2024): 22196–22197, available at <https://www.federalregister.gov/documents/2024/03/29/2024-06547/request-for-information-responsible-procurement-of-artificial-intelligence-in-government>.
- 77 Legal Information Institute, "40 U.S. Code 101 - Purpose"; Legal Information Institute, "40 U.S. Code 121(a) - Administrative."
- 78 Contractors Association of Eastern Pennsylvania v. Secretary of Labor, U.S. Court of Appeals for the 3rd Circuit, 442 F.2d 159 (April 22, 1971), available at <https://casetext.com/case/contractors-assn-v-secretary>.
- 79 American Federation of Labor and Congress of Industrial Organizations v. Kahn, U.S. Court of Appeals for the District of Columbia Circuit, 618 F.2d 784 (June 22, 1979), available at <https://casetext.com/case/american-federation-of-labor-etc-v-kahn>.
- 80 Building and Construction Trades Department, AFL-CIO v. Allbaugh, U.S. Court of Appeals for the District of Columbia Circuit, 295 F.3d 28 (July 12, 2002), available at <https://casetext.com/case/building-and-const-trades-dept-v-allbaugh>.
- 81 UAW-Labor Employment and Training Corporation v. Chao, U.S. Court of Appeals for the District of Columbia Circuit, 325 F.3d 360 (April 22, 2003), available at <https://casetext.com/case/uaw-labor-employment-and-training-v-chao>.
- 82 Legal Information Institute, "48 C.F.R. § 52.203-13 (b)(3)(i) - Contractor Code of Business Ethics and Conduct," available at <https://www.law.cornell.edu/cfr/text/48/52.203-13> (last accessed May 2024).
- 83 Ibid., § 52.203-13(c).
- 84 Legal Information Institute, "48 C.F.R. § 22.1802 - Policy," available at <https://www.law.cornell.edu/cfr/text/48/22.1802> (last accessed May 2024).
- 85 Legal Information Institute, "48 CFR § 52.203-16 - Preventing Personal Conflicts of Interest," available at <https://www.law.cornell.edu/cfr/text/48/52.203-16> (last accessed May 2024).
- 86 Executive Office of the President, "Executive Order 13706: Establishing Paid Sick Leave for Federal Contractors," Federal Register 80 (175) (2015): 54697–54700, available at <https://www.federalregister.gov/documents/2015/09/10/2015-22998/establishing-paid-sick-leave-for-federal-contractors>; Wage and Hour Division, Department of Labor, "Establishing Paid Sick Leave for Federal Contractors," Federal Register 81 (190) (2016): 67598–67724, available at <https://www.federalregister.gov/documents/2016/09/30/2016-22964/establishing-paid-sick-leave-for-federal-contractors>.
- 87 Executive Office of the President, "Executive Order 14042: Ensuring Adequate COVID Safety Protocols for Federal Contractors," Federal Register 86 (177) (2021): 50985–50989, available at <https://www.federalregister.gov/documents/2021/09/14/2021-19924/ensuring-adequate-covid-safety-protocols-for-federal-contractors>; Executive Office of the President, "Executive Order 14026: Increasing the Minimum Wage for Federal Contractors," Federal Register 86 (82) (2021): 22835–22838, available at <https://www.federalregister.gov/documents/2021/04/30/2021-09263/increasing-the-minimum-wage-for-federal-contractors>; Wage and Hour Division, "Minimum Wage for Federal Contracts Covered by Executive Order 14026, Notice of Rate Change in Effect as of January 1, 2023," Federal Register 87 (182) (2022): 59464–59468, available at <https://www.federalregister.gov/documents/2022/09/30/2022-20906/minimum-wage-for-federal-contracts-covered-by-executive-order-14026-notice-of-rate-change-in-effect>. This rule has been subject to litigation, discussed further in the "Federal contracting" section of this chapter.

- 88 Commonwealth v. Biden, U.S. Court of Appeals for the 6th Circuit, 57 F.4th 545 (January 12, 2023), available at <https://caselaw.findlaw.com/court/us-6th-circuit/2160776.html>; State of Louisiana v. Biden, U.S. Court of Appeals for the 5th Circuit, 55 F.4th 1017 (April 5, 2022), available at <https://www.ca5.uscourts.gov/opinions/pub/22/22-30087-CV0.pdf>; State of Georgia v. President of the United States, U.S. Court of Appeals for the 11th Circuit, 46 F.4th 1283 (August 26, 2022), available at <https://law.justia.com/cases/federal/appellate-courts/ca11/21-14269/21-14269-2022-08-26.html>; Mayes v. Biden, U.S. Court of Appeals for the 9th Circuit, 67 F.4th 921 (April 19, 2023), available at <https://casetext.com/case/mayes-v-biden>; State of Texas v. Biden, civil action complaint, U.S. District Court for the Southern District of Texas, Victoria Division, 6:22-CV-00004 (September 26, 2023), available at <https://cases.justia.com/federal/district-courts/texas/txsdce/6:2022-cv00004/1860274/67/0.pdf?ts=1695831032>.
- 89 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," p. 24.
- 90 Acquisition.gov, "Federal Acquisition Regulatory Council: FAR Council Members," available at <https://www.acquisition.gov/far-council-members> (last accessed February 2024).
- 91 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
- 92 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- 93 Young, "M-24-10 Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."
- 94 Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights."
- 95 National Institute for Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)" (Washington: U.S. Department of Commerce, 2023), available at <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>.
- 96 U.S. Equal Employment Opportunity Commission, "Artificial Intelligence and Algorithmic Fairness Initiative," available at <https://www.eeoc.gov/ai> (last accessed February 2024).
- 97 Emilia F. Vignola and others, "Workers' Health under Algorithmic Management: Emerging Findings and Urgent Research Questions," *International Journal of Environmental Research and Public Health* 20 (2) (2023): 1239, available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9859016/>.
- 98 Chamber of Commerce of U.S. v. Napolitano, U.S. District Court for the District of Maryland, 648 F. Supp. 2d 726, 738 (August 25, 2009), available at <https://casetext.com/case/chamber-of-commerce-of-us-v-napolitano>.
- 99 Ibid.
- 100 Ibid.
- 101 Executive Office of the President, "Executive Order 10925: Nondiscrimination in defense contracts," *Federal Register* 6 (125) (1977): 3109–3110, available at https://archives.federalregister.gov/issue_slide/1941/6/27/3109-3110.pdf#page=1 (has not been challenged); Executive Office of the President, "Executive Order 11246: Equal Employment Opportunity," *Federal Register* 30 (187) (1965): 12315–12378, available at https://archives.federalregister.gov/issue_slide/1965/9/28/12315-12325.pdf (required affirmative steps for construction contractors to root out discrimination, but its later disclosure requirements were invalidated by Chrysler); Office of Federal Contract Compliance Programs, "Discrimination on the Basis of Sex," *Federal Register* 81 (115) (2016): 39107–39169, available at <https://www.federalregister.gov/documents/2016/06/15/2016-13806/discrimination-on-the-basis-of-sex#citation-80-p3>; Congressional Research Service, "Presidential Authority to Impose Requirements on Federal Contractors," July 18, 2012, p. 7, available at https://www.everycrsreport.com/files/20120718_R41866_ad922652ef365696ef16056b2445a1babf834e5a.pdf.
- 102 Executive Office of the President, "Executive Order 14042: Ensuring Adequate COVID Safety Protocols for Federal Contractors" (revoked by Executive Order 14099); Executive Office of the President, "Executive Order 14099: Moving Beyond COVID-19: Vaccination Requirements for Federal Workers," *Federal Register* 88 (93) (2023): 30891–30892, available at <https://www.federalregister.gov/documents/2023/05/15/2023-10407/moving-beyond-covid-19-vaccination-requirements-for-federal-workers>.
- 103 Commonwealth v. Biden; State of Louisiana v. Biden; State of Georgia v. President of the United States; Mayes v. Biden.
- 104 Executive Office of the President, "Executive Order 14026: Increasing the Minimum Wage for Federal Contractors."
- 105 Bradford v. U.S. Department of Labor, U.S. District Court for the District of Colorado, 582 F. Supp. 3d 819 (January 24, 2022), available at <https://casetext.com/case/bradford-v-us-dept-of-labor-2>; State of Arizona v. Walsh, U.S. District Court for the District of Arizona, CV-22-00213-PHX-JJT (January 6, 2023), available at <https://law.justia.com/cases/federal/district-courts/arizona/azdce/2:2022-cv00213/1287218/64/>.
- 106 State of Texas v. Biden, civil action complaint, U.S. District Court for the Southern District of Texas, Victoria Division, 6:22-CV-00004 (September 26, 2023), available at <https://cases.justia.com/federal/district-courts/texas/txsdce/6:2022-cv00004/1860274/67/0.pdf?ts=1695831032>.
- 107 Bradford v. Biden, U.S. Court of Appeals for the 10th Circuit, No. 22-1023 (April 30, 2024), p. 21, available at: <https://www.ca10.uscourts.gov/sites/ca10/files/opinions/010111040629.pdf#page=21>.
- 108 State of Louisiana v. Biden, p. 1030–1033.
- 109 State of Texas v. Biden, p. 15.
- 110 Legal Information Institute, "50 U.S. Code § 4555 - Investigations; records; reports; subpoenas; right to counsel," available at <https://www.law.cornell.edu/uscode/text/50/4555> (last accessed May 2024).
- 111 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Section 4.2(a).
- 112 Ibid.
- 113 Tate Ryan-Mosley and Melissa Heikkilä, "Three things to know about the White House's executive order on AI," *MIT Technology Review*, October 30, 2023, available at <https://www.technologyreview.com/2023/10/30/1082678/three-things-to-know-about-the-white-houses-executive-order-on-ai/>.
- 114 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Section 4.2(b).
- 115 Legal Information Institute, "50 U.S.C. § 4555(a) - Investigations; records; reports; subpoenas; right to counsel."
- 116 Legal Information Institute, "50 U.S.C. § 4552(14) - Definitions," available at <https://www.law.cornell.edu/uscode/text/50/4552#14> (last accessed May 2024).
- 117 Ibid., § 4552(2).
- 118 Ibid., § 4555(d).
- 119 Executive Office of the President, "Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Section 3(k). Per the executive order, "[t]he term 'dual-use foundation model' means an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters."
- 120 Ryan-Mosley and Heikkilä, "Three things to know about the White House's executive order on AI."

- 121 L. Elaine Halchin, "National Emergency Powers" (Washington: Congressional Research Service, 2019), available at <https://crsreports.congress.gov/product/pdf/RL/98-505/11>.
- 122 Ibid.
- 123 Felix Salmon, "AI will be at the center of the next financial crisis, SEC chair warns," Axios, August 12, 2023, available at <https://www.axios.com/2023/08/12/artificial-intelligent-stock-market-algorithms>.
- 124 Office of Sen. Mark R. Warner, "Warner, Kennedy Introduce Legislation to Require Financial Regulators to Respond to AI Market Threats," Press release, December 19, 2023, available at <https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=D5D7EA33-1B34-473B-9D28-16EFBF64C7C0>.
- 125 Gregory C. Allen, "Statement before the Senate Homeland Security and Governmental Affairs Subcommittee on Emerging Threats and Spending Oversight: Advanced Technology: Examining Threats to National Security," Center for Strategic and International Studies, September 19, 2023, available at <https://www.csis.org/analysis/advanced-technology-examining-threats-national-security>.
- 126 Executive Office of the President, "Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."
- 127 The White House, "Roadmap for Researchers on Priorities Related to Information Integrity Research and Development" (Washington: 2022), available at <https://www.whitehouse.gov/wp-content/uploads/2022/12/Roadmap-Information-Integrity-RD-2022.pdf>.
- 128 Cybersecurity and Infrastructure Security Agency, "Mis-, Dis-, and Malinformation," available at https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf (last accessed February 2024).
- 129 Christopher A. Mouton, "ChatGPT Is Creating New Risks for National Security," RAND, July 20, 2023, available at <https://www.rand.org/pubs/commentary/2023/07/chatgpt-is-creating-new-risks-for-national-security.html>.
- 130 Clint Watts, "Russian US election interference targets support for Ukraine after slow start," Microsoft, April 17, 2024, available at <https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deep-fakes-ai/>; Microsoft Threat Analysis Center, "Nation-states engage in US-focused influence operations ahead of US presidential election" (Redmond: 2024), available at <https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2024/04/MTAC-Report-Elections-Report-Nation-states-engage-in-US-focused-influence-operations-ahead-of-US-presidential-election-04172024.pdf>; Clint Watts, "China tests US voter fault lines and ramps AI content to boost its geopolitical interests," Microsoft, April 4, 2024, available at <https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/>; Microsoft Threat Intelligence, "Same targets, new playbooks: East Asia threat actors employ unique methods" (Redmond: 2024), available at <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf>; Clint Watts, "Iran accelerates cyber ops against Israel from chaotic start," Microsoft, February 6, 2024, available at <https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/>; Avril Haines, "An Update on Foreign Threats to the 2024 Elections, Senate Select Committee on Intelligence," May 15, 2024, available at <https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2024/3823-dni-haines-opening-statement-as-delivered-to-the-ssci-for-an-update-on-foreign-threats-to-the-2024-elections>.
- 131 Vera Bergengruen, "Inside the Kremlin's Year of Ukraine Propaganda," Time, February 22, 2023, available at <https://time.com/6257372/russia-ukraine-war-disinformation/>.
- 132 Haines, "An Update on Foreign Threats to the 2024 Elections, Senate Select Committee on Intelligence."
- 133 U.S. Department of Defense, "Strategy for Operations in the Information Environment" (Washington: 2016), available at <https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf>; Jaspreet Gill, "Pentagon chief AI officer 'scared to death' of potential for AI in disinformation," Breaking Defense, May 3, 2023, available at <https://breakingdefense.com/2023/05/pentagon-chief-ai-officer-scared-to-death-of-potential-for-ai-in-disinformation/>.
- 134 Chief Digital and Artificial Intelligence Office, "U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway" (Washington: 2022), available at https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf.
- 135 Kathleen Hicks, "What the Pentagon Thinks About Artificial Intelligence," Politico, June 15, 2023, available at <https://www.politico.com/news/magazine/2023/06/15/pentagon-artificial-intelligence-china-00101751>.
- 136 Executive Office of the President, "Executive Order 14105: Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern," Federal Register 88 (154) (2023): 54867-54872, available at <https://www.federalregister.gov/documents/2023/08/11/2023-17449/addressing-united-states-investments-in-certain-national-security-technologies-and-products-in>.
- 137 Ibid.
- 138 Ibid.; Investment Security Office, Department of the Treasury, "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern," Federal Register 88 (154) (2023) 54961-54972, available at <https://www.federalregister.gov/documents/2023/08/14/2023-17164/provisions-pertaining-to-us-investments-in-certain-national-security-technologies-and-products-in>; Emily Benson and Gregory C. Allen, "A New National Security Instrument: The Executive Order on Outbound Investment," Center for Strategic and International Studies, August 10, 2023, available at <https://www.csis.org/analysis/new-national-security-instrument-executive-order-outbound-investment>; Tom Best and others, Paul Hastings LLP, "New U.S. Outbound Investment Restrictions on High-Technology Sectors in China," JD Supra, August 11, 2023, available at <https://www.jdsupra.com/legalnews/new-u-s-outbound-investment-5617206/>.
- 139 Evelyn Cheng, "Chinese chip stocks tumble after U.S. calls for new curbs on high-end tech," CNBC, October 10, 2022, available at <https://www.cnbc.com/2022/10/10/chinese-chip-stocks-tumble-after-us-calls-for-new-curbs-on-high-end-tech.html>; Bureau of Industry and Security, "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)," Press release, October 7, 2022, available at <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file>.
- 140 Bureau of Industry and Security, "Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections," Federal Register 88 (205) (2023): 73458-73517, available at <https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3369-88-fr-73458-acs-ifr-10-25-23/file>.
- 141 The White House, "Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Section 4.3.
- 142 Ibid., Section 4.4.
- 143 Ibid., Section 4.8.
- 144 Executive Office of the President, "Executive Order 14105: Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern."
- 145 Executive Office of the President, "Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain," Federal Register 84 (96) (2019): 22689-22692, available at <https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain>.

- 146 Executive Office of the President, "Executive Order 14034: Protecting Americans' Sensitive Data From Foreign Adversaries," Federal Register 86 (11) (2021): 31423–31426, available at <https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries>.
- 147 Executive Office of the President, "Executive Order 14117: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," Federal Register 89 (42) (2024): 15421–15430, available at <https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related>.
- 148 The White House, "FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data," February 28, 2024, available at <https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/>.
- 149 Jennifer K. Elsea, "Definition of National Emergency under the National Emergencies Act" (Washington: Congressional Research Service, 2019), available at <https://crsreports.congress.gov/product/pdf/LSB/LSB10267>. There are several theories as to what constitutes a "national emergency" within the meaning of the National Emergencies Act. Legal Information Institute, "50 U.S. Code § 1621(a) - Declaration of national emergency by President; publication in Federal Register; effect on other laws; superseding legislation," available at <https://www.law.cornell.edu/uscode/text/50/1621> (last accessed May 2024).
- 150 Christopher A. Casey, Dianne E. Rennack, and Jennifer K. Elsea, "The International Emergency Economic Powers Act: Origins, Evolution, and Use" (Washington: Congressional Research Service, 2024), available at <https://sgp.fas.org/crs/natsec/R45618.pdf>. Congress enacted the IEEPA to regularize presidents' use of exigent economic-based sanctions.
- 151 Ibid.
- 152 Legal Information Institute, "50 U.S.C. § 1701 - Unusual and extraordinary threat; declaration of national emergency; exercise of Presidential authorities," available at <https://www.law.cornell.edu/uscode/text/50/1701> (last accessed May 2024).
- 153 Legal Information Institute, "50 U.S.C. § 1702(b) - Presidential authorities," available at <https://www.law.cornell.edu/uscode/text/50/1702> (last accessed May 2024). The statute exempts, subject to some exceptions, from the president's emergency authority the power to "regulate or prohibit, directly or indirectly:" personal communications that do not involve the transfer of value; humanitarian donations; importation or exportation of educational materials; and personal effects and remittances. Other IEEPA exemptions, generally known as the "Berman Amendment," exempt importation or exportation "of any information or informational materials." The administration may face litigation for taking action on AI, depending on the breadth of emergency action. TikTok challenged the Trump administration's attempted use of IEEPA against it and won a preliminary injunction. The case was later dismissed when the Biden administration rescinded the Trump administration's executive action. See Stephen P. Mulligan, "Restricting TikTok (Part I): Legal History and Background" (Washington: Congressional Research Service, 2023), available at <https://crsreports.congress.gov/product/pdf/LSB/LSB10940>; Mike Isaac and David McCabe, "TikTok Wins Reprieve From U.S. Ban," The New York Times, September 27, 2020, available at <https://www.nytimes.com/2020/09/27/technology/tiktok-ban-ruling-app.html>; Brian Fung, "TikTok, Biden administration agree to drop litigation over Trump-era app store ban," CNN, July 22, 2021, available at <https://www.cnn.com/2021/07/22/tech/tiktok-trump-ban-dismissed/index.html>.
- 154 Legal Information Institute, "50 U.S.C. § 1702(a)(1) – Presidential authorities." This authorizes the president, in the event of a declared national emergency, to "investigate, regulate, or prohibit – (i) any transactions in foreign exchange, (ii) transfers of credit or payments between, by, through, or to any banking institution, to the extent that such transfers or payments involve any interest of any foreign country or a national thereof, (3) the importing or exporting of currency or securities, by any person, or with respect to any property, subject to the jurisdiction of the United States" and to "investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States."
- 155 Legal Information Institute, "50 U.S.C. § 1708(b) - Actions to address economic or industrial espionage in cyberspace," available at <https://www.law.cornell.edu/uscode/text/50/1708> (last accessed May 2024).
- 156 Legal Information Institute, "47 U.S.C. § 606(d) - War powers of President," available at <https://www.law.cornell.edu/uscode/text/47/606> (last accessed May 2024). "Upon proclamation by the President that there exists a state or threat of war involving the United States, the President ... may ... (1) suspend or amend the rules and regulations applicable to any or all facilities or stations for wire communication within the jurisdiction of the United States as prescribed by the Commission, (2) cause the closing of any facility or station for wire communication and the removal therefrom of its apparatus and equipment, or (3) authorize the use or control of any such facility or station and its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners."
- 157 Federal Procurement Policy, "41 U.S.C. Subtitle I - Federal Procurement Policy," § 3304, available at <https://www.law.cornell.edu/uscode/text/41/3304> (last accessed May 2024).
- 158 Joshua L. Friedman, "Emergency Powers of the Executive: The President's Authority When All Hell Breaks Loose," *Journal of Law and Health* 25 (2) (2012): 265–306, available at https://www.law.csuohio.edu/sites/default/files/academics/jlh/friedman_final_version_of_article-2.pdf.
- 159 See *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (June 2, 1952), available at <https://supreme.justia.com/cases/federal/us/343/579/> (establishing an influential tripartite framework for the scope of inherent presidential authority in the context of various congressional postures).
- 160 Adam Conner, "The Needed Executive Actions to Address the Challenges of Artificial Intelligence" (Washington: Center for American Progress, 2023), available at <https://www.americanprogress.org/article/the-needed-executive-actions-to-address-the-challenges-of-artificial-intelligence/>; Megan Shahi and Adam Conner, "Priorities for a National AI Strategy," Center for American Progress, August 10, 2023, available at <https://www.americanprogress.org/article/priorities-for-a-national-ai-strategy/>.
- 161 Executive Office of the President, "Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Section 4.8.
- 162 Friedman, "Emergency Powers of the Executive: The President's Authority When All Hell Breaks Loose." President George W. Bush issued Homeland Security Presidential Directive 5, which called for the creation of the National Response Plan. The National Response Plan, most recently reissued as the National Response Framework, was designed to guide scenario planning for a variety of disasters, including a biological, nuclear, or radiological accident or terrorist attack; a natural disaster, such as a tsunami, hurricane, fire, or earthquake; a malicious cyberattack; a food and agriculture disaster involving the nation's food and/or agriculture supply; an incident involving oil and/or hazardous materials and pollution; a biological health quarantine; or a terrorist attack not involving any of the above.

- 163 Friedman, "Emergency Powers of the Executive: The President's Authority When All Hell Breaks Loose."
- 164 Legal Information Institute, "50 U.S.C. Chapter 35 - International Emergency Economic Powers," § 1701 et. seq., available at <https://www.law.cornell.edu/uscode/text/50/chapter-35> (last accessed May 2024).
- 165 Casey, Rennack, and Elsea, "The International Emergency Economic Powers Act: Origins, Evolution, and Use," p. 26. "[N]o President has used IEEPA to enact a policy that was primarily domestic in effect. Some scholars argue, however, that the interconnectedness of the global economy means it would probably be permissible to use IEEPA to take an action that was primarily domestic in effect."
- 166 See Legal Information Institute, "47 U.S.C. § 606(c) - War powers of President." Upon "proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States," the president may suspend or amend regulations applicable to any or all stations or devices capable of emitting electromagnetic radiation and may cause the closing of any radio station. And per 47 U.S.C. § 606(d), "[U]pon proclamation by the President that there exists a state or threat of war involving the United States, the President ... may ... (1) suspend or amend the rules and regulations applicable to any or all facilities or stations for wire communication within the jurisdiction of the United States as prescribed by the Commission, (2) cause the closing of any facility or station for wire communication and the removal therefrom of its apparatus and equipment, or (3) authorize the use or control of any such facility or station and its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners."
- 167 Government of Canada, "Everyday things that emit radiation," available at <https://www.canada.ca/en/health-canada/services/health-risks-safety/radiation/everyday-things-emit-radiation.html> (last accessed February 2024); Michael J. Socolow, "In a State of Emergency, the President Can Control Your Phone, Your TV, and Even Your Light Switches," Reason Magazine, February 15, 2019, available at <https://reason.com/2019/02/15/in-a-state-of-emergency-the-president-ca/>.
- 168 Legal Information Institute, "41 U.S.C. Subtitle I - Federal Procurement Policy," § 3304 (authorizing agencies to use noncompetitive procurement procedures if "it is necessary to award the contract to a particular source or sources in order ... to maintain a facility, producer, manufacturer, or other supplier available for furnishing property or services in case of a national emergency or to achieve industrial mobilization").
- 169 The president could also consider action under the Trade Expansion Act. For example, the president could restrict – via tariffs or otherwise – imports of inputs to AI applications, such as semiconductors, when doing so would protect national security. Subject to certain preconditions, the act allows the president to "determine the nature and duration of the action that, in the judgment of the President, must be taken to adjust the imports of the article and its derivatives so that such imports will not threaten to impair the national security" and, in some cases, "take such other actions as the President deems necessary to adjust the imports" of certain articles if the commerce secretary finds that the quantity or manner in which they are imported impairs national security. See Legal Information Institute, "19 U.S.C. § 1862(b)-(c) - Safeguarding national security," available at <https://www.law.cornell.edu/uscode/text/19/1862> (last accessed May 2024).