FACT SHEET

Recommendations for the White House To Take Further Action on AI

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

This fact sheet collects the recommendations from Chapter 1: "The White House" of the joint report from Governing for Impact (GFI) and the Center for American Progress, "Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authorities To Regulate Artificial Intelligence." The chapter notes how the White House and its subordinate agencies, including the Office of Management and Budget (OMB) and the Office of Information and Regulatory Affairs (OIRA), should consider addressing potential artificial intelligence (AI) risks and opportunities beyond the October 2023 "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."[1] The White House 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 do so. The goal of these recommendations is to provoke a generative discussion about the following proposals, rather than outline a definitive executive action agenda. This menu of potential recommendations demonstrates that there are more options for agencies to explore beyond their current work, and that agencies should immediately utilize existing authorities to address AI.

Read the full report

Taking Further Agency Action on AI

Read the full chapter

The White House

The Office of Management and Budget

Uniform guidance for federal awards

The OMB could consider the following actions:

- **Develop guidance that adapts the recent OMB M-24-10 AI guidance[2] 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 guidance[3] 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."[4] 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.

Updates to regulatory review

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,[5] 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,[6] 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,[7] 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,[8] 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

Federal procurement policy and Federal Property and Administrative Services Act (FPASA)

As the OMB prepares the forthcoming procurement guidance mentioned in OMB M-24-10 AI guidance,[9] 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,[10] 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.[11]
- **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.

The Executive Office of the President

International Emergency Economic Powers Act (IEEPA), the Communications Act, and Federal Procurement Policy

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.[12] 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.[13] 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.[14]
  - **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.[15] 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.[16]

- **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.[17] The bounds of this authority are quite broad, covering an enormous number of everyday devices, including smartphones that can emit electromagnetic radiation.[18]
- **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.[19]
- **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.[20] 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.

Endnotes

1 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.

2 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.

3 Ibid., Appendix I.

4 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).

5 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.

6 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.

7 Executive Office of the President, "Executive Order 14110: 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."

8 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. 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)," available at https://www.hhs.gov/sites/default/files/department-of-health-and-human-services-omb-m-21-06.pdf (last accessed 2024); 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.

9 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.

10 Acquisition.gov, "Federal Acquisition Regulatory Council: FAR Council Members," available at https://www.acquisition.gov/far-council-members (last accessed February 2024).

11 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."

12 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.

13 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.

14 Friedman, "Emergency Powers of the Executive: The President's Authority When All Hell Breaks Loose."

15 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).

16 Cristopher 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.

17 See 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).

18 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/.

19 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).

20 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).

FACT SHEET

Recommendations for the Department of Labor To Take Further Action on AI

By Reed Shaw

Read the full report

Taking Further Agency Action on AI

Read the full chapter

The Department of Labor

This fact sheet collects the recommendations from Chapter 2: "The Department of Labor" of the joint report from Governing for Impact (GFI) and the Center for American Progress, "Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authorities To Regulate Artificial Intelligence." The chapter notes how the U.S. Department of Labor (DOL) oversees numerous statutes, from the Fair Labor Standards Act (FLSA) to the Family and Medical Leave Act (FMLA), that can potentially help address the challenges and opportunities of artificial intelligence (AI) as it affects workers. These recommendations stem from DOL-enforced statutes identified in the chapter that could be used to address AI through regulations, subregulatory guidance, and enforcement practices. Among other authorities, the DOL could use these statutes to ameliorate known harms by updating wage and hour regulations, guarding workers' safety and health against the negative impacts of automated management, and ensuring that automated benefits administration is transparent and fair. The goal of these recommendations is to provoke a generative discussion about the following proposals, rather than outline a definitive executive action agenda. This menu of potential recommendations demonstrates that there are more options for agencies to explore beyond their current work, and that agencies should immediately utilize existing authorities to address AI.

Fair Labor Standards Act: Recordkeeping and reporting

Based on this authority, the DOL could consider the following actions:

- **Issue new recordkeeping and reporting rules**, pursuant to 29 U.S.C. § 211(c), to require employer records to ensure legibility and transparency of wage determinations made by automated systems and to require periodic reports to the Wage and Hour Division (WHD) of those records from employers using AI-driven wage and scheduling technology. Such regulations would help combat black-box wage determination and discrimination[1] that can make workers' wages unpredictable and irregular,[2] as well as ensure that such wage determinations

satisfy the minimum wage and overtime requirements of the FLSA. As documented by Veena Dubal, professor of law at the University of California, Irvine, many workers are subject to algorithmic management and wage setting that withholds or reduces compensation for work when doing so benefits the company.[3] This can make it difficult for workers to appreciate the connection between time spent working and amount of income generated, or to understand and correct errors in their compensation, and can also result in opaque wage setting that violates minimum wage or overtime laws.[4] The DOL contemplated a similar rulemaking in the early 2010s that would have required recordkeeping and disclosure to workers about their status as employees or independent contractors and detailed information about how their pay is computed, but a regulation was never proposed.[5]

- **Launch investigations**, pursuant to its administrative subpoena power in 29 U.S.C. § 211(a),[6] of employers to ensure compliance with minimum wage and overtime provisions. The WHD could prioritize investigation of employers that are noncompliant with the reporting rules mentioned, are in industries with large numbers of employee complaints, or are in industries with high penetration of automated wage and scheduling technologies. These investigations could produce valuable information about the characteristics of automated systems that make minimum wage and overtime violations more likely to occur and encourage employers' compliance with their legal obligations under the FLSA.

Fair Labor Standards Act: Minimum wage and overtime

Based on the above-cited authority, the DOL could consider the following action:

- **Issue updated interpretive regulations at 29 C.F.R. Part 785,** pursuant to 29 U.S.C. § 211(c), that allow only employers who track time manually through analog methods to engage in timesheet rounding[7] and establish a presumption against application of the de minimis rule in cases where employers use highly precise timekeeping technology.[8] These changes would eliminate an outdated regulatory regime that allows companies to use sophisticated timekeeping technology to facilitate wage theft by exploiting rules meant to minimize the burden of pen-and-paper wage and hour calculations. Given the ubiquity and ease of digital timekeeping, there is no longer a compelling justification for allowing practices such as rounding employees' hours to the nearest quarter-hour or failing to treat short periods of working time as compensable for minimum wage and overtime compliance.[9]

Unemployment compensation

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

- **Update quality control program regulations at 20 CFR § 602.21,** pursuant to 42 U.S.C. §§ 503(a)(1) and 1302, to require states to undertake audits and submit their results to the DOL for any automated or AI-driven benefits determination

system. This could help ensure that states provide unemployment compensation to individuals consistent with federal law, provide for human in-the-loop review of any algorithmic denial of benefits, and ensure fair human adjudication for appeals of those denials. The current quality control program regulations were promulgated based on this same statutory authority.[10] These regulations would guard against states' use of automated systems to deny coverage to eligible individuals (or worse, wrongfully accuse them of fraud),[11] a use case cited by the Office of Management and Budget (OMB) as presumptively rights-impacting, and therefore it should be subject to heightened scrutiny.[12] This proposal is closely related to the actions directed in Section 7.2(b) of the president's 2023 executive order on AI, which aims to ensure the equitable distribution of public benefits. For example, the executive order directs the U.S. Department of Agriculture to issue guidance to state, local, and Tribal governments that address the use of AI systems in benefits distribution. It requires such guidance to ensure that such systems, among other things, maximize program access; require governments to notify the Department of Agriculture of AI use; create opt-out opportunities for benefit denial appeal; and enable auditing to ensure equitable outcomes.[13]

- **Issue a new unemployment insurance program letter (UIPL)** to guide states specifically on where and how AI can and should be implemented for unemployment insurance administration. This new UIPL should incorporate the minimum risk management practices for the presumed rights-impacting use of AI from the OMB M-24-10 AI memo[14] and any subsequent guidance. For example, utilizing AI to flag potential fraud must be accompanied by the minimum risk practices from the OMB M-24-10 AI memo, such as carrying out AI impact assessments, testing the systems in the real world before widespread deployment, and ongoing monitoring to ensure equity.[15] The DOL should clarify that these requirements extend to any vendor a state unemployment insurance system contracts with to provide services.

Occupational Safety and Health Act

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

- **Begin the standard-setting process,** pursuant to 29 U.S.C. § 655(b), to regulate the use of electronic surveillance and automated management (ESAM) in the workplace to the extent that it creates hazards to workers' physical and mental safety and health. Such regulation could mitigate the increasingly unsustainable pace of work enforced by these systems, which leads to ergonomic injury and increased risk of accidents. For example, the Washington State Department of Labor and Industries has fined Amazon repeatedly for forcing its warehouse workers to work at punishing speeds that exacerbate the risk of injury.[16] The state's citations specifically reference the "direct connection" between Amazon's ESAM and workplace musculoskeletal disorders.[17] A standard on ESAM would also reduce the harmful effects that these systems can have on workers' mental health. As

early as 1987, the now-defunct U.S. Office of Technology Assessment recognized that ESAM increases employee stress, heightening job strain risk.[18]

Of course, the Occupational Safety and Health Administration's (OSHA) standard-setting process is uniquely slow and resource intensive for the agency,[19] and the process would need to be informed by additional research to design an effective policy. So, in the meantime, the following recommendations should be considered:

- **Issue new subregulatory guidance and bring general duty clause enforcement** actions related to companies' use of ESAM in ways that harm worker safety and health. As GFI has urged in past advocacy efforts, OSHA should follow the lead of Washington state by more directly tying ESAM use to physical and mental health hazards.[20] Enforcement actions based on unsafe ESAM use could be taken because of the already ongoing DOL investigation into high injury rates at Amazon warehouses.[21]

- **Update existing subregulatory guidance about sector-specific ergonomic risks** to include a discussion of how ESAM can increase musculoskeletal injury risk. As described in a GFI report in 2023, OSHA could update the ergonomics guidance documents for poultry processing and grocery warehousing and create a new ESAM-conscious ergonomic risks guidance document for the warehousing industry.[22] The guidance could describe best practices to prevent ergonomic injuries—such as quota transparency, worker involvement in quota setting, and rest breaks—and how ESAM systems should be adjusted to accommodate those best practices.

- **Update injury reporting regulations at 29 C.F.R. Part 1904,** pursuant to 29 U.S.C. § 657, revising OSHA's log of work-related injuries and illnesses (Form 300) to collect information about automated systems used in the tasks, job roles, or workplaces in which the worker was working at the time of injury or illness. Additionally, OSHA could update Form 300 to include a column identifying when injuries are musculoskeletal.[23] This would allow OSHA to develop a better understanding of the precise causal mechanisms between ESAM and these injuries and inform the substantive policymaking described above.

- **Request research from the National Institute for Occupational Safety and Health,** pursuant to 29 U.S.C. § 671(d), to fund and conduct further research to study ESAM's effect on job strain and physical injury.[24]

Employee Retirement Income Security Act: Adverse benefits determination and disclosure

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

- **Update regulations at 29 C.F.R. § 2560.503-1,** which implement the denial-of-claims disclosure and appeal requirements at 29 U.S.C. § 1133. The current regulations state, for example, that in the case of an adverse benefit determination by a group health plan, a participant is entitled to request a copy of any "internal rule, guideline, protocol, or other similar criterion" that was relied on in making the adverse determination.[25] An updated regulation could require affirmative disclosure of a plain-language description of any algorithmic determination involved in a benefits determination, as well as the results of an equity audit conducted in a manner similar to that recommended in the OMB M-24-10 AI memo.[26] Additionally, the updated regulations could clarify that the appeal process authorized by 29 U.S.C. § 1133(2) and outlined at 29 C.F.R. § 2560.503-1(h) requires that appeals of benefits denials be heard by a human. This update could come as part of the DOL's announced review of the Employee Retirement Income Security Act (ERISA) disclosures pursuant to the Setting Every Community Up for Retirement Enhancement (SECURE) Act 2.0.[27]

- **Update regulations at 29 C.F.R. § 2520.102-3(l)** to amend the summary of plan description to include a plain language description of any automated and algorithmic systems that the plan uses to make determinations that could "result in disqualification, ineligibility, or denial or loss of benefits,"[28] as well as whether the system has been externally audited or the administrator has instituted safeguards such as opt-out mechanisms for participants who would prefer human-made determinations. This would provide some transparency to workers and advocates about the decisions that plan administrators make with the help of AI-driven systems. This update could also come as part of the DOL's announced review of ERISA disclosures pursuant to the SECURE Act 2.0.[29]

Employee Retirement Income Security Act: Investment advice

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

- **Update regulations at 29 C.F.R. § 2550.404a-1(c),** pursuant to 29 U.S.C. § 1104, to revise the investment duty of loyalty in light of the risks that AI-driven investment allocation technologies can create and potential conflicts of interest. The updated regulation could be similar to the U.S. Securities and Exchange Commission's rulemaking proceedings that seek to prevent investment advisers from using algorithms that create conflicts of interest between the adviser and the investor's retirement goals.[30] Importantly, plan fiduciaries should be required to ensure that AI-driven investment advice or allocations are not improperly weighted toward decisions that maximize fees and commissions at the expense of retirement savers. Such regulations could also require an audit of any AI-driven or otherwise

automated investment allocation technologies for the potential for conflicts of interest.

- **Issue new regulations,** pursuant to 29 U.S.C. § 1104(c)(5), requiring algorithmic transparency and legibility to plan participants and beneficiaries for default asset allocations.[31]

- **Update the statutory transactions exemption at 29 C.F.R. § 2550.408g-1(b)(4),** "Arrangements that use computer models," to strengthen the existing auditing requirements and institute other AI-specific requirements, taking into account the DOL's approach in the proposed revisions to the Prohibited Transaction Exemption 2020-02.[32] Alternatively, or in addition to updating the exemption, the DOL could issue guidance that more fully describes the term "computer model" and identifies AI applications to which this exemption may apply.

Labor Management Reporting and Disclosure Act

Based on the above-cited authority, the DOL could consider the following action:

- **Issue a regulation or subregulatory guidance,** in the form of independent guidance documents or in the LM-10 form instructions, that explains how forms of ESAM can chill workers' exercise of their Section 7 rights under the National Labor Relations Act and when they must be reported in employers' LM-10 forms. The use of worker surveillance to thwart organizing activities is well-documented.[33] The regulation or guidance could explain how that might require employers to report their expenditures on such technologies. They could reference the memo issued by the National Labor Relations Board's general counsel on the subject,[34] as well as prior guidance from the DOL on surveillance reporting.[35] Additional guidance may empower workers, unions, and labor watchdogs to report employer noncompliance to the DOL.

Worker Adjustment and Retraining Notification Act

Based on the above-cited authority, the DOL could consider the following action:

- **Update regulations at 20 C.F.R. § 639.3(i)**, pursuant to 29 U.S.C. § 2107(a), to explain that, in the case of a completely or primarily remote workforce, the term "single site of employment" applies to the employer's entire workforce. In the case of algorithmic management, the DOL should clarify that all workers subject to the same or similar algorithm are considered one single site of employment. Updated regulations could also ensure that workers subject to intermittent deplatforming caused by algorithmic optimization have maximal protections possible under the Worker Adjustment and Retraining Notification (WARN) Act.

Family and Medical Leave Act

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

- **Update regulations at 29 C.F.R. Part 825,** pursuant to 29 U.S.C. §§ 2615(a)(1) and 2654, to require legibility and transparency of automated systems[36] that make any determinations bearing on the allocation or approval of FMLA leave, along with any other applicable minimum practices for rights-impacting AI from the OMB M-24-10 AI memo.[37] This would implement the transparency protections recommended by the White House's AI Bill of Rights and ensure that employers' use of automated systems does not unlawfully restrain workers' exercise of their rights under the FMLA. Because FMLA determination algorithms are likely bound up in other human resource management systems, this proposal could also provide transparency of those benefits processes as well. Specifically, these updated regulations should require:
  - At 29 C.F.R. § 825.301, legibility and transparency around use of automated systems to make FMLA designations
  - Legibility and transparency around use of automated systems to review, request, or otherwise process certifications under 29 U.S.C. § 2613
  - Legibility and transparency around use of automated systems to provide eligibility notices, at 29 C.F.R § 825.300(b); rights and responsibilities notices, at 29 C.F.R. § 825.300(c); and designation notices, at 29 C.F.R. § 825.300(d)
  - At 29 C.F.R. § 825.302, legibility and transparency around use of automated systems for employees to provide notice of the use of leave or to transmit information around scheduling of intermittent leave under 9 U.S.C. § 2612(b) and (e)

- **Update regulations by modifying 29 C.F.R. § 825.220,** pursuant to 29 U.S.C. §§ 2615(a)(1) and 2654, to prohibit employers from using FMLA data as inputs to any automated management system that may make an employment decision based, in part, on an employee's use or nonuse of FMLA leave. This would reduce employers' ability to weaponize employees' data against them to retaliate for using FMLA leave. Under these recommended updated regulations, the automated management system must strictly segregate and keep confidential any information provided for FMLA certification pursuant to 29 C.F.R. § 825.500(g).

- **Update subregulatory guidance under 29 C.F.R. § 825.301(a)** prohibiting automated systems from using information other than that received from the employee or the employee's authorized spokesperson in designating FMLA leave pursuant to 29 C.F.R. § 825.301(a). Existing regulation already prohibits the conduct for employers and would also apply to automated systems used by employers, but additional clarification is essential to restrict automated systems that would improperly combine data sources.

Endnotes

1 Veena Dubal, "The House Always Wins: the Algorithmic Gamblification of Work," LPE Project, January 23, 2023, available at https://lpeproject.org/blog/the-house-always-wins-the-algorithmic-gamblification-of-work/.

2 For example, in one 2017 lawsuit against Uber, a class of drivers alleged that there was a discrepancy between their contracted rate (a fixed proportion of an often-inflated rider's fare payment) and their actual rate (a backend mileage- and time-based rate), which resulted in systematic underpayment and breach of contract. See Dulberg v. Uber Technologies Inc. and Rasier, class action complaint, U.S. District Court for the Northern District of California, 3:17-cv-00850 (February 21, 2017), available at https://www.classaction.org/media/dulberg-v-uber.pdf.

3 Many are misclassified as independent contractors and may be beyond the reach of the FLSA, though the DOL's new rulemaking on independent contractor versus employee status will reduce the severity of misclassification.

4 See Dubal, "The House Always Wins: The Algorithmic Gamblification of Work." See also Zephyr Teachout, "Surveillance Wages: A Taxonomy," LPE Project, November 6, 2023, available at https://lpeproject.org/blog/surveillance-wages-a-taxonomy/.

5 Office of Information and Regulatory Affairs, "Right to Know Under the Fair Labor Standards Act," available at https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201404&RIN=1235-AA04 (last accessed May 2024); Office of Information and Regulatory Affairs, "Right to Know Under the Fair Labor Standards Act," available at https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201104&RIN=1235-AA04 (last accessed May 2024).

6 See U.S. Department of Justice, "Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities" (Washington: 2002), available at https://www.justice.gov/archive/olp/rpt_to_congress.htm#1a for a thorough discussion of administrative subpoena powers held by executive agencies.

7 Legal Information Institute, "29 C.F.R. § 785.48(b) - Use of time clocks," available at https://www.law.cornell.edu/cfr/text/29/785.48 (last accessed May 2024).

8 Legal Information Institute, "29 C.F.R. § 785.47 - Where records show insubstantial or insignificant periods of time," available at https://www.law.cornell.edu/cfr/text/29/785.47 (last accessed May 2024).

9 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; Charlotte S. Alexander and Elizabeth Tippett, "The Hacking of Employment Law," Missouri Law Review 82 (4) (2017): 973–1022, p. 990, available at https://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=4299&context=mlr.

10 See U.S. Department of Labor, "Final Rule, Federal-State Unemployment Compensation Program; Unemployment Insurance Quality Control Program," Federal Register 52 (171) (1987): 33506–33522, available at https://archives.federalregister.gov/issue_slice/1987/9/3/33506-33533.pdf.

11 See, for example, Robert N. Charette, "Michigan's MiDAS Unemployment System: Algorithm Alchemy Created Lead, Not Gold," IEEE Spectrum, January 24, 2018, available at https://spectrum.ieee.org/michigans-midas-unemployment-system-algorithm-alchemy-that-created-lead-not-gold.

12 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), Appendix I, 2.I., p. 33, 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.

13 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, at Section 7.2(b), available at https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

14 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," at 5.c., pp. 15–24.

15 Ibid., at 5.c.iv.A.,5.c.iv.B and 5.c.i.v.C, pp. 17–23.

16 Lauren Rosenblatt, "Fine with fines? Amazon isn't making enough changes to protect warehouse workers, Washington state says," Tech Xplore, March 29, 2022, available at https://techxplore.com/news/2022-03-fine-fines-amazon-isnt-warehouse.html.

17 Washington State Department of Labor and Industries, "Citation and Notice: Amazon Com Services," May 4, 2021, available at https://s3.documentcloud.org/documents/20787752/amazon-dupont-citation-and-notice-may-2021.pdf.

18 Office of Technology Assessment, "The Electronic Supervisor: New Technology, New Tensions" (Washington: U.S. Government Printing Office, 1987), available at https://ota.fas.org/reports/8708.pdf. See, generally, Governing for Impact and Center for Democracy and Technology, "Memos to the White House and federal agencies," April 3, 2023, available at https://governingforimpact.org/wp-content/uploads/2023/04/Surveillance_Package.pdf.

19 David Michaels and Jordan Barab, "The Occupational Safety and Health Administration at 50: Protecting Workers in a Changing Economy," American Journal of Public Health 110 (5) (2020): 631–635, available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7144438/; U.S. Government Accountability Office, "Report to Congressional Requesters: Workplace Health and Safety: Multiple Challenges Lengthen OSHA's Standard Setting" (Washington: 2012), available at https://www.gao.gov/assets/gao-12-330.pdf.

20 Governing for Impact and Center for Democracy and Technology, "Memos to the White House and federal agencies."

21 U.S. Department of Labor, "US Department of Labor finds Amazon exposed workers to unsafe conditions, ergonomic hazards at three more warehouses in Colorado, Idaho, New York," Press release, February 1, 2023, available at https://www.osha.gov/news/newsreleases/national/02012023. While making up roughly one-third of the national warehouse workforce, Amazon workers account for 49 percent of all warehouse injuries in the country. See Mitchell Clark, "Amazon workers made up almost half of all warehouse injuries last year," The Verge, April 12, 2022, available at https://www.theverge.com/2022/4/12/23022107/amazon-warehouse-injuries-us-half.

22 Governing for Impact and Center for Democracy and Technology, "Memos to the White House and federal agencies."

23 See U.S. Department of Labor, "US Labor Department's OSHA temporarily withdraws proposed column for work-related musculoskeletal disorders, reaches out to small businesses," Press release, January 25, 2011, available at https://www.osha.gov/news/newsreleases/national/01252011; Occupational Safety and Health Administration, "Occupational Injury and Illness Recording and Reporting Requirements" (Washington: U.S. Department of Labor, 2003), available at https://www.osha.gov/laws-regs/federalregister/2003-06-30.

24 Governing for Impact and Center for Democracy and Technology, "Memos to the White House and federal agencies," 02-1.

25 Legal Information Institute, "29 C.F.R. § 2560.503-1(g)(1) - Claims procedure," available at https://www.law.cornell.edu/cfr/text/29/2560.503-1 (last accessed May 2024).

26 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," at 5.c.v.A., p. 21.

27 Office of Information and Regulatory Affairs, "Improving Participant Engagement and Effectiveness of ERISA Retirement Plan Disclosures," available at https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=1210-AC09 (last accessed May 2024).

28 Legal Information Institute, "29 U.S.C. § 1022(b) - Summary plan description," available at https://www.law.cornell.edu/uscode/text/29/1022 (last accessed May 2024).

29 Office of Information and Regulatory Affairs, "Improving Participant Engagement and Effectiveness of ERISA Retirement Plan Disclosures."

30 U.S. Securities and Exchange Commission, "Fact Sheet: Conflicts of Interest and Predictive Data Analytics" (Washington: 2023), available at https://www.sec.gov/files/34-97990-fact-sheet.pdf.

31 Amy Caiazza, Rob Rosenblum, and Danielle Sartain, "Investment Advisers' Fiduciary Duties: The Use of Artificial Intelligence," Harvard Law School Forum on Corporate Governance, June 11, 2020, available at https://corpgov.law.harvard.edu/2020/06/11/investment-advisers-fiduciary-duties-the-use-of-artificial-intelligence/.

32 Employee Benefits Security Administration, "Proposed Amendment to Prohibited Transaction Exemption 2020-02," Federal Register 88 (212) (2023): 75979–76003, available at https://www.federalregister.gov/documents/2023/11/03/2023-23780/proposed-amendment-to-prohibited-transaction-exemption-2020-02; Fred Reish, "The New Fiduciary Rule (8): Special Issues – Robo Advice and Investment Education," JD Supra, December 4, 2023, available at https://www.jdsupra.com/legalnews/the-new-fiduciary-rule-8-special-issues-9929375/.

33 See, for example, Jo Constantz, "'They Were Spying On Us': Amazon, Walmart, Use Surveillance Technology to Bust Unions," Newsweek, December 13, 2021, available at https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603; Indigo Oliver, "McDonald's spies on union activists – that's how scared they are of workers' rights," The Guardian, March 2, 2021, available at https://www.theguardian.com/commentisfree/2021/mar/02/mcdonalds-unions-workers-rights#:~:text=This%20includes%20using%20data%20collection,the%20Chicago%20and%20London%20offices%E2%80%9D.&text=This%20comes%20after%20years%20of,unionization%20of%20their%20o.

34 National Labor Relations Board, "NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices," Press release, October 31, 2022, available at https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and.

35 U.S. Department of Labor, "OLMS Fact Sheet: Form LM-10 Employer Reporting Transparency Concerning Persuader, Surveillance, and Unfair Labor Practice Expenditures" (Washington: 2022), available at https://www.dol.gov/sites/dolgov/files/OLMS/regs/compliance/LM10_FactSheet.pdf?_ga=2.185647721.1329945632.1706553922-76066306.1688999107; Jeffrey Freund, "How We're Ramping Up Our Enforcement of Surveillance Reporting," U.S. Department of Labor Blog, September 15, 2022, available at https://blog.dol.gov/2022/09/15/how-were-ramping-up-our-enforcement-of-surveillance-reporting.

36 See, for example, Ecotime by HBS, "Ensure Time-Savings and Compliance With FMLA Software," available at https://ecotimebyhbs.com/solutions/fmla/ (last accessed February 2024).

37 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."

FACT SHEET

Recommendations for the Department of Education To Take Further Action on AI

By Anna Rodriguez

This fact sheet collects the recommendations from Chapter 3: "Department of Education" of the joint report from Governing for Impact (GFI) and the Center for American Progress, "Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authorities To Regulate Artificial Intelligence." The chapter notes how the U.S. Department of Education should consider addressing potential artificial intelligence (AI) risks to education using existing statutory authorities in titles VI and IX of the Civil Rights Act, the Americans with Disabilities Act (ADA), and the Higher Education Act (HEA).[1] These statutes can be used to address impermissible discrimination using AI technology and provide various requirements for contractors servicing student loans. The goal of these recommendations is to provoke a generative discussion about the following proposals, rather than outline a definitive executive action agenda. This menu of potential recommendations to address AI demonstrates that there are more options for agencies to explore beyond their current work and that agencies should immediately utilize existing authorities to address AI.

Read the full report

Taking Further Agency Action on AI

Read the full chapter

Department of Education

Title VI of the Civil Rights Act of 1964

- **Issue guidance under Title VI explaining that 34 C.F.R. Part 100 applies to discrimination enabled by AI or other generative technology.** Specifically, this guidance would include examples of impermissible discrimination using AI technology, including disproportionate discipline for students of color, students with disabilities, or students for whom English is not their first language.

Title IX of the Civil Rights Act of 1964

- **Issue guidance specifying that, under 34 C.F.R. 106.31(b), using AI or other automated technologies, including generative AI, may violate Title IX if it results in sex discrimination.** This includes discriminatory surveillance of students because of their sex, disparate discipline resulting from that surveillance, or the filtering out of appropriate internet content because of discriminatory or imprecise AI internet monitoring.

Americans with Disabilities Act, Section 504 of the Rehabilitation Act, and the Individuals with Disabilities Education Act

- **Issue guidance explaining the Americans with Disabilities Act's application to AI's discriminatory effects in surveillance and discipline,** including specific examples of possible discriminatory effects of programs that detect AI-generated work or cheating. The guidance could also address how some students may benefit from AI-assisted programs, which can constitute an accommodation in certain circumstances.

Higher Education Act

- **Require that contracted servicers using AI-generated chatbots ensure that borrowers are receiving accurate information about their individual loans.** This includes an option to speak with a human within a reasonable amount of time and incorporating any of the relevant minimum risk management practices for rights-impacting purposes developed through the Office of Management and Budget (OMB) M-24-10 memorandum on "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."[2]

Endnotes

1 Legal Information Institution, "42 U.S.C. § 2000d et seq. Prohibition against exclusion from participation in, denial of benefits of, and discrimination under federally assisted programs on ground of race, color, or national origin," Title VI, available at https://www.law.cornell.edu/uscode/text/42/2000d (last accessed May 2024); Legal Information Institute, "20 U.S.C. § 1681 et seq. - Sex," Title IX, available at https://www.law.cornell.edu/uscode/text/20/1681 (last accessed May 2024); U.S. Government Publishing Office, "42 U.S.C. § 126 et seq. Equal Opportunity for Individuals with Disabilities," available at https://uscode.house.gov/view.xhtml?path=/prelim@title42/chapter126&edition=prelim (last accessed May 2024); Higher Education Act, Public Law 329, 89th Cong., 1st sess. (November 8, 1965), as amended, available at https://www.govinfo.gov/content/pkg/COMPS-765/pdf/COMPS-765.pdf.

2 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), p. 32, 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.

FACT SHEET

Recommendations for Housing Regulators To Take Further Action on AI

By Anna Rodriguez

This fact sheet collects the recommendations from Chapter 4: "Housing Regulators" of the joint report from Governing for Impact (GFI) and the Center for American Progress, "Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authorities To Regulate Artificial Intelligence." The chapter notes how the U.S. Department of Housing and Urban Development (HUD) and other housing regulators should consider addressing potential artificial intelligence (AI) risks to housing fairness and discrimination using existing statutory authorities in the Fair Housing Act (FHA) and the Dodd-Frank Wall Street Reform and Consumer Protection Act. The goal of these recommendations is to provoke a generative discussion about the following proposals, rather than outline a definitive executive action agenda. This menu of potential recommendations to address AI demonstrates that there are more options for agencies to explore beyond their current work and that agencies should immediately utilize existing authorities to address AI.

Read the full report

Taking Further Agency Action on AI

Read the full chapter

Housing Regulators

Fair Housing Act

Based on FHA authorities, HUD could take the following action:

- **Update the "Fair Housing Advertising" guidelines – a separate document from the newly released advertising guidance – elucidating Section 804(c)'s prohibition against discrimination in the advertisement of housing opportunities in the context of online advertising that relies on algorithmic tools or data,** as required by the 2023 "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" and consistent with the recent HUD guidance on advertising through digital platforms.[1] Such guidance would be consistent with the U.S. Department of Justice's (DOJ) settlement with Facebook, which targeted similar practices,[2] and can specifically highlight practices that lead to housing advertisements being steered away from protected communities.[3] Furthermore, the guidance should specify that companies providing advertising services using AI technologies are liable. The guidelines should mirror the responsibilities and liabilities outlined in HUD's recent guidance.[4]

Dodd-Frank Act

Based on this authority, the Federal Housing Finance Agency (FHFA) should take the following actions:

- **Continue the rulemaking process on the proposed automated valuation model (AVM) rule but also include its application to all mortgage lenders**—specifically nonbanks, given that more than half of annual residential real estate loans were made by nonbanks in 2022.[5] Furthermore, the rule should include specific minimum standards for each proposed goal, potentially incorporating the National Institute of Standards and Technology (NIST) AI guidelines[6] or relevant minimum standards developed in response to the minimum risk management practices anticipated by the Office of Management and Budget (OMB) M-24-10 memorandum on "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence."[7]

- **Specify, through the proposed AVM rule or additional rulemaking, that companies using AVMs must disclose their use to customers and allow customers to request nonautomated appraisals or seek valuation from alternative AVMs.** The FHFA can do so using its broad authority in Section 1125 to "account for any other such factor that the agencies ... determine to be appropriate."[8] This would align with the statute's purpose to "ensure a high level of confidence in [AVMs]," "protect against the manipulation of data," and "avoid conflict of interest."[9]

Endnotes

1 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; Office of Fair Housing and Equal Opportunity, "Guidance on Application of the Fair Housing Act to the Advertising of Housing, Credit, and Other Real Estate-Related Transactions through Digital Platforms" (Washington: U.S. Department of Housing and Urban Development, 2024), available at https://www.hud.gov/sites/dfiles/FHEO/documents/FHEO_Guidance_on_Advertising_through_Digital_Platforms.pdf; American Civil Liberties Union and others, "Re: Addressing Technology's Role in Housing Discrimination," July 13, 2021, available at https://www.upturn.org/static/files/letter-to-ostp-on-housing-technologies-20210713.pdf; Office of Fair Housing and Equal Opportunity, "Part 109--Fair Housing Advertising," available at https://www.hud.gov/sites/dfiles/FHEO/documents/BBE%20Part%20109%20Fair%20Housing%20Advertising.pdf (last accessed March 2024).

2 Office of Public Affairs, "Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising," Press release, U.S. Department of Justice, June 21, 2022, available at https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.

3 See, for example, Harlan Yu, Aaron Rieke, and Natasha Duarte, "Urging the Biden Administration to Address Technology's Role in Housing Discrimination," Upturn, July 13, 2021, available at https://www.upturn.org/work/proposals-for-the-biden-administration-to-address-technology-housing/.

4 Office of Fair Housing and Equal Opportunity, "Guidance on Application of the Fair Housing Act to the Advertising of Housing, Credit, and Other Real Estate-Related Transactions through Digital Platforms."

5 Dennis Kelleher, "Re: Quality Control Standards for Automated Valuation Models – OCC Docket ID OCC – 2023-0002; Board Docket No. R-1807 and RIN No. 7100 AG60; FDIC RIN 3064-AE68; NCUA Docket Number NCUA-2023-0019 and RIN 3133-AE23; CFPB Docket No. CFPB-2023-0025; FHFA RIN 2590-AA62; 88 Fed. Reg. 40638 (Jun. 21, 2023)," Better Markets, August 21, 2023, available at https://www.regulations.gov/comment/OCC-2023-0002-0011. See Rica Dela Cruz and Gaby Villaluz, "Nonbank lenders shed mortgage market share as originations plummet in 2022," S&P Global, July 13, 2023, available at https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/nonbank-lenders-shed-mortgage-market-share-as-originations-plummet-in-2022-76481554.

6 National Institute of Standards and Technology, "NIST AI RMF Playbook," available at https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook (last accessed February 2024).

7 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.

8 Legal Information Institute, "12 U.S.C. § 3354 - Automated valuation models used to estimate collateral value for mortgage lending purposes," available at https://www.law.cornell.edu/uscode/text/12/3354 (last accessed May 2024). See, for example, Alexei Alexandrov, Laurie Goodman, and Michael Neal, "Reengineering the Appraisal Process: Better Leveraging Both Automated Valuation Models and Manual Appraisals" (Washington: Urban Institute, 2023), p. 18, available at https://www.urban.org/sites/default/files/2023-01/Reengineering%20the%20Appraisal%20Process.pdf.

9 Legal Information Institute, "12 U.S.C. § 3354(a)(1)–(3)."

FACT SHEET

Recommendations for Financial Regulatory Agencies To Take Further Action on AI

By Todd Phillips and Adam Conner

This fact sheet collects the recommendations from Chapter 5: "Financial Regulatory Agencies" of the joint report from Governing for Impact (GFI) and the Center for American Progress, "Taking Further Agency Action on AI: How Agencies Can Deploy Existing Statutory Authorities To Regulate Artificial Intelligence." The chapter notes how artificial intelligence (AI) is poised to affect every aspect of the U.S. economy and play a significant role in the U.S. financial system, leading financial regulators to take various steps to address the impact of AI on their areas of responsibility. The impacts of AI on consumers, banks, nonbank financial institutions, and the financial system's stability are all concerns to be investigated and potentially addressed by regulators using numerous existing authorities. The goal of these recommendations is to provoke a generative discussion about the following proposals, rather than outline a definitive executive action agenda. This menu of potential recommendations demonstrates that there are more options for agencies to explore beyond their current work, and that agencies should immediately utilize existing authorities to address AI.

Read the full report

Taking Further Agency Action on AI

Read the full chapter

Financial Regulatory Agencies

In this fact sheet, the term "U.S. financial regulatory agencies" includes the federal banking and credit union agencies, financial markets regulators, and executive branch agencies. Specifically, in this fact sheet, these agencies include the Treasury Department, the Office of the Comptroller of the Currency (OCC); the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation (FDIC); the Commodity Futures Trading Commission (CFTC); the National Credit Union Administration (NCUA); the Securities and Exchange Commission (SEC); the Consumer Financial Protection Bureau (CFPB); the Financial Stability Oversight Council (FSOC), which is chaired by the secretary of the treasury; and, to some extent, the Financial Industry Regulatory Authority (FINRA), the self-regulatory organization for securities brokers, which is overseen by the SEC. It should be noted that other federal agencies not listed here also have financial regulation responsibilities and authorities that could potentially be used to address AI.

Bank Secrecy Act

Relevant agencies: *Treasury Department, Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Commodity Futures Trading Commission*

Using this authority, the Federal Reserve, OCC, FDIC, SEC, and CFTC could consider the following actions:

- **Regulate how institutions' customer identification and suspicious activity reporting programs use AI.** As AI becomes more integrated into financial systems, it can help institutions monitor and analyze transactions for Bank Secrecy Act (BSA) compliance more effectively, detecting anomalies or patterns indicative of illicit activities. However, regulators must be cognizant of the harms of offloading such an important law enforcement task to AI systems and should outline best practices for implementing AI systems and require institutions to develop standards for how they use AI to automate anti-money laundering tasks.

- **Require banks to periodically review their BSA systems to ensure accuracy and explainability.** Accurate and timely reports of suspicious activities must be balanced against financial privacy and the Financial Crimes Enforcement Network's ability to review the reports it receives. Regulators must ensure the AI institutions' BSA systems use is accurate and can explain why activities are suspicious and therefore flagged. Regulators should require institutions to periodically review their AI—perhaps by hiring outside reviewers—to ensure continued accuracy and explainability to expert and lay audiences. Examiners must be able to review source code and dataset acquisition protocols.

Gramm-Leach-Bliley Act: Disclosure of nonpublic personal information

Relevant agencies: *Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration, Securities and Exchange Commission, Commodity Futures Trading Commission, Consumer Financial Protection Bureau*

The regulators should make further use of this authority to ensure resiliency against AI-designed cyber threats, including the following actions:

- **Require third-party AI audits for all institutions.** AI audits should be required for all institutions. Larger institutions can bring this practice in-house, depending on the ecosystem that develops around AI audits. However, smaller financial institutions may lack the staff and funding for in-house expertise or AI red-teaming but still need to mitigate AI risk. Accordingly, small institutions should undergo AI security

audits by qualified outside consultants to determine where vulnerabilities lie. These audits help identify and address any vulnerabilities in AI systems that might be exploited by cyber threats, thus enhancing overall cybersecurity measures. This includes risks that cybercriminals could use AI to impersonate clients such that institutions inadvertently release customer information erroneously, believing that they are interacting with their clients. Regulators should set out guidelines for appropriate conflict checks and firewall protocols for auditors.

- **Require red-teaming of AI for the largest institutions.** AI red-teaming is defined as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI."[1] The largest firms should already be utilizing red-teaming for their AI products. In addition, they should be running red team/blue team exercises, and the agencies should require the teams to incorporate AI into their efforts. Using AI can significantly increase the speed at which red teams can find and exploit vulnerabilities, leaving blue teams at a significant disadvantage.[2] Firms must know how malicious actors can use AI to attack their infrastructure to defend against it effectively. Banks and other financial institutions must conduct AI red-teaming to fortify their cyber defenses and proactively identify vulnerabilities.

- **Require disclosure of annual resources on AI cybersecurity and AI risk management and compliance.** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance, which is crucial for transparency and accountability. Given the escalating reliance on AI-driven technologies in banking operations, the potential vulnerabilities and risks associated with cyber threats amplify significantly. By mandating such disclosures, stakeholders, including customers, regulators, and investors, gain valuable insights into a bank's commitment to mitigating cyber risks through AI.

Equal Credit Opportunity Act

Relevant agency: *Consumer Financial Protection Bureau*

Using this authority, the CFPB could consider the following actions:

- **Require lenders to periodically review their lending systems to ensure explainability and that no new discriminatory activity applies.** Research suggests that AI-based systems may result in lending decisions that have a disparate impact,[3] which is a violation of the Equal Credit Opportunity Act (ECOA).[4] The CFPB has already indicated in guidance that AI-based lending systems cannot be used when those systems "cannot provide the specific and accurate reasons for adverse actions."[5] Nevertheless, the CFPB should require lenders making lending decisions using AI to periodically review those systems—perhaps by hiring

outside reviewers—to ensure explainability to expert and lay audiences and to confirm that discrimination does not inadvertently creep in as new data are used. Examiners must review source code and dataset acquisition protocols.

- **Prohibit lenders from using third-party credit scores and models developed with unexplainable AI.** Many lenders use credit scores or other sources of information from third parties, which themselves may use AI to create those ratings.[6] The CFPB should prohibit lenders from using unexplainable scores or models to avoid fair lending requirements and require all lenders subject to the ECOA to obtain information about the explainability of their third-party service providers' AI.

- **Require lenders to employ staff with AI expertise.** As described above, many lenders rely on third-party models for lending decisions. Given the pitfalls of algorithmic lending decisions, these firms must maintain diverse teams that include individuals with AI expertise to understand how such models operate and can introduce bias into firms' lending decisions. These experts are necessary to identify and mitigate potential biases or unintended consequences of algorithmic decision-making. The 2023 executive order on AI required federal agencies to appoint chief artificial intelligence officers (CAIOs),[7] whose duties were further outlined in the OMB M-24-10 AI guidance.[8] The CFPB should follow that model to require firms to similarly designate a CAIO or designate an existing official to assume the duties of a CAIO.

Fair Credit Reporting Act

Relevant agency: *Consumer Financial Protection Bureau*

As it relates to AI, the CFPB should consider using this authority to take the following actions:

- **Require credit reporting agencies to describe whether and to what extent AI was involved in formulating reports and scores.** Although the CFPB has issued guidance making clear that the ECOA requires lenders to make their AI systems explainable,[9] it has yet to do the same with credit reporting agencies. Given that AI-based systems may result in the creation of credit scores that will result in a disparate impact, the CFPB should use its authority over credit reporting agencies to make clear that the AI used to generate credit scores should describe the extent to which AI was used and ensure the scores are explainable.

- **Require credit reporting agencies to periodically review their AI systems to ensure explainability and that no new discriminatory activity applies.** Beyond simply requiring credit reporting agencies' AI systems to be explainable to expert and lay audiences, the CFPB should also require the agencies to periodically

review their systems to ensure continued explainability as new data are introduced. CFPB examiners must be able to review source code and dataset acquisition protocols.

- **Require credit reporting agencies to provide for human review of information that consumers contest as inaccurate.** As part of the U.S.C. § 1681i "reasonable reinvestigation" mandate, credit reporting agencies should be required to have a human conduct the reinvestigation of AI systems' determinations and inputs.[10] Since AI-based systems may use black-box algorithms to determine credit scores or inputs that create credit scores, individually traceable data are required for adequate human review. As noted above, general explainability is important but would not be sufficient to allow human reviewers to correct potentially erroneous information under the Fair Credit Reporting Act (FCRA).

- Given the preceding recommendation, **require users of credit reports to inform consumers of their right to human review of inaccuracies in AI-generated reports in adverse action notices,** per 15 U.S.C. § 1681(m)(4)(B).

- **Update model forms and disclosures to incorporate disclosure of AI usage.** Given the CFPB's mandate that credit reporting agencies and users of credit reports use model forms and disclosures, the CFPB should update those forms to include spaces for model form users to describe their AI usage.

Importantly, "consumer reports" under the FCRA include those that provide information used "in establishing the consumer's eligibility for ... employment purposes."[11] "Employment purposes" include the "purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee."[12] The CFPB should consider several policy changes to explicitly address electronic surveillance and automated management (ESAM) used by employers:

- **Require purveyors of workplace surveillance technologies to comply with the FCRA.** As AI firms become increasingly used to mine data provided by employers, it is important that ESAM software companies be considered credit reporting agencies and comply with the corresponding restrictions. The CFPB should consider adding such companies to its list of credit reporting agencies[13] and issue supervisory guidance explaining the circumstances under which ESAM companies act as credit reporting agencies and the corresponding responsibilities that they entail for ESAM companies and employers.

- **Ensure ESAM technologies used by employers comply with the FCRA.** If the CFPB provides that these technology providers are credit reporting agencies, the CFPB must also make clear that users of their software comply with the FCRA. Accordingly, the CFPB should consider modifying its "Summary of Consumer Rights" to include information about employee FCRA rights concerning

employers' use of ESAM technologies.[14] It should also consider modifying "Appendix E to Part 1022" to identify how employers furnishing employee data to ESAM technology companies and data brokers must ensure the accuracy of their furnished information.[15]

Community Reinvestment Act

Relevant agencies: *Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation*

The federal banking regulators should consider using their authority to:

- **Require banks to indicate whether they use AI to comply with Community Reinvestment Act (CRA) regulations and, if so, require those systems to be explainable.** Given AI systems' abilities to wade through mountains of information and identify the most profitable outcomes, banks may use them to game CRA regulations. For example, banks may use AI to help determine the most optimal assessment areas for profitability purposes. Regulators should require banks to disclose if they use AI to comply with the CRA or with regulations promulgated thereunder. In addition, these AI systems should be required to be explainable to expert and lay audiences to ensure that designated assessment areas are logical. Examiners must be able to review source code and dataset acquisition protocols.

Consumer Financial Protection Act: UDAAP authority

Relevant agency: *Consumer Financial Protection Bureau*

Using this authority, the CFPB should consider the following actions:

- **Require financial institutions' consumer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict consumer protection standards, periodically reviewing consumer-facing AI systems to ensure accuracy and explainability.** As institutions begin using AI chatbots to communicate with customers, these systems must provide consumers with accurate information about their accounts, their firms' policies and procedures, and the law. In addition, as these AI systems begin to be used for more than simply providing information—such as executing customers' money transfers or asset purchases—it is imperative that they accurately and effectively execute transactions according to customers' wishes and execute only transactions that are legal and comply with firms' policies. The CFPB must ensure that institutions' consumer-facing AI systems are accurate in all respects and require, through rulemaking, periodic review of their systems to ensure accuracy.

- **Require AI red-teaming and red team/blue team exercises for the largest institutions.** The CFPB's unfair, deceptive, or abusive acts or practices (UDAAP) authority can be used to prohibit the inadvertent disclosure of consumers' information at institutions not subject to the Gramm-Leach-Bliley Act.[16] Nonbank consumer financial service providers hold a wealth of information about customers off of which malicious AI systems feed, and they may be liable for customer losses stemming from AI-enabled fraud.[17] With AI red-teaming[18] or red team/blue team exercises, the red team attempts to attack a company's information technology infrastructure while the blue team defends against such hacks. The largest firms should already be utilizing AI red-teaming and red team/blue team exercises, but given that real-world attackers have AI at their disposal, the agencies should require this. Having teams use AI can significantly increase the speed with which red teams can find and exploit vulnerabilities, leaving blue teams at a significant disadvantage.[19] Firms must understand how malicious actors can use AI to attack their infrastructure and defend against it. Institutions must conduct AI red-teaming and red team/blue team exercises leveraging AI to fortify their cyber defenses and proactively identify vulnerabilities.

- **Require third-party AI audits for all institutions.** AI audits should be required by all institutions. Larger institutions can bring this practice in-house, depending on the ecosystem that develops around AI audits. However, smaller financial institutions may lack the staff and funding for in-house expertise or AI red-teaming or red team/blue team exercises[20] but still need to mitigate AI risk. Accordingly, small institutions should be required to undergo AI security audits by outside consultants to determine where vulnerabilities lie. These audits help identify and address any vulnerabilities in AI systems that might be exploited by cyber threats, thus enhancing overall cybersecurity measures. The CFPB may require such audits because failure to do so while claiming accurate and secure systems is unfair. Regulators should set guidelines for appropriate conflict checks and firewall protocols for auditors.

- **Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.** Requiring nonbank consumer financial service providers to disclose their annual resources dedicated to cybersecurity and AI risk management and compliance is crucial for transparency and accountability. Given the escalating reliance on AI-driven technologies in financial institution operations,[21] the potential vulnerabilities and risks associated with cyber threats amplify significantly. The CFPB could enact regulations mandating such resource disclosures for spending on cybersecurity and AI risk management and compliance. By mandating such disclosures, stakeholders, including customers, regulators, and investors, would gain valuable insights into the extent of an institution's commitment to mitigating cyber risks through AI.

Federal Deposit Insurance Act, Federal Credit Union Act, and Bank Holding Company Act

Relevant agencies: *Federal Reserve, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration*

Using these authorities, the Federal Reserve, FDIC, OCC, and NCUA should consider the following actions:

- **Require financial institutions' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict standards, and require those institutions to periodically review their customer-facing AI systems to ensure accuracy and explainability.** As institutions begin using AI chatbots to communicate with customers, these systems provide customers with accurate information about their accounts, their firms' policies and procedures, and the law. In addition, as these AI systems begin to be used for more than simply providing information—such as executing customers' money transfers or asset purchases—it is imperative that they accurately and effectively execute transactions according to customers' wishes and execute only transactions that are legal and within firms' policies. Regulators must ensure that institutions' customer-facing AI systems are accurate and require periodic reviews of their systems to ensure accuracy.

- **Ensure banks' capital structures can withstand sudden and deep withdrawals of customer deposits or losses from banks' risk management processes.** Banks' corporate clients are likely to begin using AI systems for treasury management—including bank deposits—and there are likely to be only a small number of providers of such systems, given the large computing power necessary for effective AI.[22] AI-based treasury management systems may automatically move all firms' cash, simultaneously creating significant movements of cash between financial institutions in short periods of time that result in sudden and significant drops in customer deposits. Regulators must ensure that banks maintain sufficient shareholder capital and high-quality liquid assets that enable them to withstand such shifts without failing.

- **Require that AI systems that are parts of banks' capital, investment, and other risk management models be explainable.** Banks today use various systems to automate their capital management strategies, evaluate investment opportunities, and otherwise mitigate risk. They will inevitably use AI for these and other purposes that have significant effects on their profitability and stability. The banking agencies already review firms' risk management practices regarding the various models they use, and regulators should do the same with AI. Specifically, all AI systems must be explainable to expert and lay audiences. Examiners must be allowed to review source code and dataset acquisition protocols.

- **Ensure firms may move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not develop their own systems in-house; instead, they will license software from a few competing nonfinancial institutions.[23] Financial firms must be able to move between different and competing AI systems to avoid lock-in. Accordingly, regulators should make it a prerequisite for using AI that any system adopted from a third-party service provider allows for easy transition to a competing system upon the contract's expiration. Regulators must ensure that there are many—for example, at least five—providers of AI software for banks that provide for base interoperability, so that not all institutions are using the same one or two pieces of software.

- **Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance, which is crucial for transparency and accountability. Given the escalating reliance on AI-driven technologies in banking operations, the potential vulnerabilities and risks associated with cyber threats amplify significantly. By mandating such disclosures, stakeholders, including customers, regulators, and investors, gain valuable insights into the extent of a bank's commitment to mitigating cyber risks through AI. Bank and credit union annual disclosures could provide these disclosures.

Dodd-Frank Act: Systemic risk designation

Relevant agency: *Financial Stability Oversight Council*

Using its financial market utilities (FMU) designation authority, the FSOC should consider the following actions in the event that major providers of AI services reach a level of systemic importance to warrant oversight under these authorities:

- **Designate major providers of AI services to financial institutions as systemically important if they reach an adoption level that creates vulnerability.** It may appear incongruous at first glance to designate AI service providers as not only systemically important but also as systemically important FMUs. They do not facilitate payments, are not clearinghouses, do not provide for settlement of financial transactions, nor do they engage in significant financial transactions with counterparties. However, providers of AI services to the largest and most systemically important financial institutions could still meet the FSOC's two determinations if they become so important to traders and market makers that, if the AI systems stop working for those firms, it "could create, or increase, the risk of significant liquidity or credit problems [in the markets]."[24]

Consider, for example, that market makers such as investment banks use AI systems to facilitate trades. If those systems stop working or execute faulty trades, significant liquidity could be removed from the markets, causing asset prices to drop precipitously along with financial instability. Similar arguments may be made for brokers using AI to manage their funding needs: If AI systems stop working, those brokers could lose access to funding sources, causing them to collapse. And the same is potentially true for high-frequency traders using AI to manage their trades—as faulty AI systems could result in flash crashes. Accordingly, the FSOC should monitor which AI systems are relied on by significant players in the markets and consider designating them as systemically important if their failure could threaten the stability of the U.S. financial system.

- **Designate the cloud service providers to those firms designated as systemically important.** AI systems rely on cloud service providers, such as Amazon Web Services or Microsoft Azure, to operate; thus, if these cloud providers fail, AI systems also fail.[25] Indeed, AI programs run on cloud providers' servers and require cloud providers' computing power to conduct the large-scale language processing required for AI. To the extent that AI software is of systemic importance to the financial system and may pose systemic risks if it fails, the fact that AI software cannot operate without cloud providers means that cloud providers are also of systemic importance to the financial system and may pose systemic risks themselves. This is not a new idea; members of Congress and advocacy organizations have previously called for such designation.[26] However, the rise of AI gives this proposal new urgency. Accordingly, once the FSOC identifies which AI systems are systemically important, it should determine the cloud providers on which they rely and consider designating them as systemically important.

Securities Exchange Act of 1934

Relevant agency: *Securities and Exchange Commission*

Using this authority, the SEC should consider the following actions:

- **Require that AI systems that are parts of brokers' capital, investment, and other risk management models be explainable.** Brokers use a variety of systems to automate their capital management strategies, evaluate investment opportunities, and mitigate risk. They will inevitably use AI for these and other purposes that significantly affect their profitability and stability. The SEC already regulates brokers' risk management models,[27] and it should do the same with AI. Specifically, all AI systems must be explainable to expert and lay audiences. The SEC should also ensure that it and FINRA's examiners may review source code and dataset acquisition protocols.

- **Require brokers' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards, with those brokers periodically reviewing their customer-facing AI systems to ensure accuracy and explainability.** As institutions begin using AI chatbots to communicate with customers, these systems must provide clients with accurate information about their accounts, their policies and procedures, and the law. In addition, as these AI systems are used for more than simply providing information—such as executing customer trades—it is critical that they accurately and effectively execute transactions according to customers' wishes and execute only transactions that are legal and within firms' policies. The SEC must ensure that brokers' customer-facing AI systems undergo periodic review to ensure accuracy through third-party audits.

- **Require brokers using AI systems to make investment recommendations to ensure those systems are explainable and operate in clients' best interests.** There may come a day when AI systems are used to make investment recommendations. Before that occurs, the SEC must make clear that any AI systems used for that purpose must comply with existing rules that require investment recommendations to be in clients' best interests.[28] Among other things, AI systems must be explainable to expert and lay audiences. Brokers must also be able to explain why their recommendations are not provided based on conflicts of interest. Furthermore, the SEC should require brokers using AI to make investment recommendations to periodically review those systems and ensure that examiners may review source code and dataset acquisition protocols.

- **Require red-teaming of AI for exchanges, alternative trading systems, and clearinghouses.** AI red-teaming is defined as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI."[29] The largest firms should already be utilizing red teaming for their AI products. In addition, they should be running red team/blue team exercises, and the agencies should require the teams to incorporate AI into their efforts. Using AI can significantly increase the speed with which red teams can find and exploit vulnerabilities, leaving blue teams at a significant disadvantage.[30] Firms must be aware of how malicious actors can use AI to attack their infrastructure to be able to defend against it. Banks and other financial institutions must conduct AI red-teaming to fortify their cyber defenses and proactively identify vulnerabilities. Given the systemic importance of these firms, the SEC should not allow third-party audits to suffice, but rather deploy multiple steps to ensure security and protection.

- **Ensure firms may move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not develop their own systems in-house; instead, they will license software from a few competing nonfinancial institutions.[31]

It will be imperative that financial firms be able to move between different and competing AI systems to avoid lock-in. Accordingly, the SEC should make it a prerequisite of using AI that any system adopted from a third-party service provider allows for easy transition to a competing system upon the contract's expiration. The SEC could require that brokers, exchanges, alternative trading systems, and clearinghouses ensure that there are many—for example, at least five—providers of AI software that provide for base interoperability before entering contracts, so that not all institutions are using the same one or two pieces of software.

- **Require disclosure of annual resources dedicated to cybersecurity spending and AI risk management and compliance.** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance for transparency and accountability. Given the escalating reliance on AI-driven technologies in financial services, the potential vulnerabilities and risks associated with cyber threats amplify significantly. The SEC should, accordingly, mandate brokers, exchanges, and clearinghouses to disclose their annual expenditures on cybersecurity and AI risk management and compliance. By mandating such disclosures, the SEC can gain valuable insights into the extent of a firm's commitment to mitigating AI risk management.

Investment Advisers Act of 1940

Relevant agency: *Securities and Exchange Commission*

Using this authority, the SEC should consider the following actions:

- **Require that registered investment advisers' (RIAs) AI systems used to make investment recommendations are explainable and operate in clients' best interests.** There may come a day when AI systems are used to make investment recommendations. Before that occurs, the SEC must make clear that any AI systems used for that purpose must comply with existing rules that require investment recommendations to be in clients' best interests. Among other things, RIAs' AI systems must be explainable to both expert and lay audiences and explain why their recommendations are not provided based on conflicts of interest. Furthermore, the SEC should require RIAs that use AI to make investment recommendations to periodically review those systems and ensure that examiners may review source code and dataset acquisition protocols.

- **Require RIAs' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards, with RIAs periodically reviewing their customer-facing AI systems to ensure accuracy and explainability.** As institutions begin using AI chatbots to communicate with customers, these systems provide clients with accurate information about their accounts, their firms' policies and procedures, and the

law in a manner that is not misleading. In addition, as these AI systems begin to be used for more than simply providing information—such as executing customer trades—it is imperative that they accurately and effectively execute transactions according to customers' wishes and execute only legal transactions within firms' policies. The SEC must ensure that RIAs' customer-facing AI systems are accurate and require periodic reviews of their systems to ensure accuracy.

- **Ensure RIAs may move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not be developing their systems in-house; instead, they will license software from a small number of competing nonfinancial institutions.[32] It is imperative that RIAs are able to move between different and competing AI systems to avoid lock-in. Accordingly, the SEC should make it a prerequisite for using AI that any system adopted from a third-party service provider allows for easy transition to a competing system upon the contract's expiration. The SEC must require that RIAs ensure that there are many—for example, at least five—providers of AI software that provide for base interoperability before entering contracts, so that not all institutions are using the same one or two pieces of software.

Commodity Exchange Act

Relevant agency: *Commodity Futures Trading Commission*

Using myriad authorities under the Commodity Exchange Act, the CFTC should consider the following actions:

- **Require AI systems that are parts of futures commission merchants', swap dealers', or major swap participants' capital, investment, or other risk management models to be explainable.** Today, these entities use a variety of systems to automate their capital management strategies, evaluate investment opportunities, and mitigate risk. They will inevitably begin using AI for these and other purposes that significantly affect their profitability and stability. The CFTC should regulate its AI models and ensure that all AI systems are explainable to expert and lay audiences. The CFTC should also ensure that it and the National Futures Association's examiners may review source code and dataset acquisition protocols.

- **Require futures commission merchants' customer-facing AI systems to accurately respond to customer inquiries and execute transactions subject to strict investor protection standards.** As institutions begin using AI chatbots to communicate with customers, these systems provide clients with accurate information about their accounts, their firms' policies and procedures, and the law. In addition, as these AI systems begin to be used for more than simply

providing information—such as executing customer trades—it is imperative that they accurately and effectively execute transactions according to customers' wishes and execute only transactions that are legal and within firms' policies. The CFTC must ensure that futures commission merchants' customer-facing AI systems are accurate in all respects and require periodic reviews of those systems to ensure accuracy and explainability.

- **Require that FCMs' AI systems used to make investment recommendations be explainable and operate in clients' best interests.** There may come a day when AI systems are used to make investment recommendations. Before that occurs, the CFTC must make clear that any AI systems used for that purpose must comply with existing rules that require investment recommendations to be in clients' best interests. Among other things, AI systems must be explainable to expert and lay audiences and explain why recommendations are not provided based on conflicts of interest. Furthermore, the CFTC should require FCMs using AI to make investment recommendations, to periodically review those systems, and to ensure that examiners can review source code and dataset acquisition protocols.

- **Require red-teaming of AI for swap dealers, exchanges, and clearinghouses.** AI red-teaming is defined as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI."[33] The largest firms should use red-teaming for their AI products. In addition, they should run red team/blue team exercises and require the teams to incorporate AI into their efforts. Using AI can significantly increase the speed with which red teams can find and exploit vulnerabilities, leaving blue teams at a significant disadvantage.[34] Firms must be aware of how malicious actors can use AI to attack their infrastructure to be able to defend against it. Banks and other financial institutions must conduct AI red-teaming to fortify their cyber defenses and proactively identify vulnerabilities.

- **Require third-party AI audits for all institutions.** All institutions should require AI audits. Larger institutions can bring this practice in-house, depending on the ecosystem that develops around AI audits. However, smaller financial institutions may lack the staff and funding for in-house expertise or AI red-teaming but still need to mitigate against AI risk. Accordingly, small institutions should be required to undergo AI security audits by outside consultants to determine where vulnerabilities lie. These audits help identify and address any vulnerabilities in AI systems that might be exploited by cyber threats, thus enhancing overall cybersecurity measures. Regulators should set out guidelines for appropriate conflict checks and firewall protocols for auditors.

- **Ensure firms can move between different AI systems before they contract for one system.** The sheer amount of computing power involved in generative AI means that most financial institutions will not be developing their systems in-house; instead, they will license software from a few competing nonfinancial

institutions.[35] It is imperative that financial firms are able to move between different and competing AI systems to avoid lock-in. Accordingly, the CFTC should make it a prerequisite for using AI that any system adopted from a third-party service provider allows for an easy transition to a competing system upon the contract's expiration. The CFTC must require that all registrants and registered entities ensure that there are many—for example, at least five—providers of AI software that provide for base interoperability before entering contracts, so that not all institutions use the same one or two pieces of software.

- **Require disclosure of annual resources dedicated to cybersecurity and AI risk management and compliance.** Financial institutions must disclose their annual resources dedicated to cybersecurity and AI risk management and compliance, which is crucial for transparency and accountability. Given the escalating reliance on AI-driven technologies in financial services, the potential vulnerabilities and risks associated with cyber threats amplify significantly. Accordingly, the CFTC should mandate that registrants and registered entities disclose their annual expenditures on cybersecurity and AI risk management and compliance. By mandating such disclosures, the CFTC can gain valuable insights into the extent of a firm's commitment to mitigating AI risks.

Endnotes

1 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.

2 Laiba Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?", Splunk, May 17, 2023, available at https://www.splunk.com/en_us/blog/learn/red-team-vs-blue-team.html.

3 Christine Polek and Shastri Sandy, "The Disparate Impact of Artificial Intelligence and Machine Learning," Colorado Technology Law Journal 21 (1) (2023): 85–108, available at https://ctlj.colorado.edu/wp-content/uploads/2023/08/FINAL-3-SP-6.17.23_AK-edits-3.pdf.

4 Consumer Financial Protection Bureau, "CFPB Consumer Laws and Regulations" (Washington: 2013), available at https://files.consumerfinance.gov/f/201306_cfpb_laws-and-regulations_ecoa-combined-june-2013.pdf.

5 Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms" (Washington: 2022), available at https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.

6 Giorgio Baldassarri Hoger von Hogersthal, "Artificial Intelligence and Alternative Data in Credit Scoring and Credit Risk Surveillance," S&P Global, October 10, 2023, available at https://www.spglobal.com/en/research-insights/featured/special-editorial/artificial-intelligence-and-alternative-data-in-credit-scoring-and-credit-risk-surveillance; Sally Ward-Foxton, "Reducing Bias in AI Models for Credit and Loan Decisions," EE Times, April 30, 2019, available at https://www.eetimes.com/reducing-bias-in-ai-models-for-credit-and-loan-decisions/; Louis DeNicola, "Which Credit Scores Do Mortgage Lenders Use?", Experian, April 22, 2024, available at https://www.experian.com/blogs/ask-experian/which-credit-scores-do-mortgage-lenders-use/; Datrics, "AI Credit Scoring: The Future of Credit Risk Assessment," available at https://www.datrics.ai/articles/the-essentials-of-ai-based-credit-scoring (last accessed March 2024).

7 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," 10.1(b)(i).

8 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.

9 Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2023-03: Adverse action notification requirements and the proper use of the CFPB's sample forms provided in Regulation B" (Washington: 2023), available at https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/.

10 Johnson v. MBNA America Bank, N.A., U.S. Court of Appeals for the 4th Circuit, 357 F.3d 426, 432 (February 11, 2004), available at https://casetext.com/case/johnson-v-mbna-america-bank-na (explaining that reasonableness for both kinds of investigations is determined by "weighing the cost of verifying disputed information against the possible harm to the consumer").

11 Legal Information Institute, "15 U.S. Code § 1681a(d)(1) - Definitions; rules of construction," available at https://www.law.cornell.edu/uscode/text/15/1681a#h (last accessed May 2024).

12 Legal Information Institute, "15 U.S. Code § 1681a."

13 Consumer Financial Protection Bureau, "List of Consumer Reporting Companies" (Washington: 2023), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2023.pdf.

14 Consumer Financial Protection Bureau, "Appendix K to Part 1022 - Summary of Consumer Rights," available at https://www.consumerfinance.gov/rules-policy/regulations/1022/k/ (last accessed February 2024).

15 Consumer Financial Protection Bureau, "Appendix E to Part 1022 - Interagency Guidelines Concerning the Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies," available at https://www.consumerfinance.gov/rules-policy/regulations/1022/e/ (last accessed May 2024)

16 Consumer Financial Protection Bureau, "Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information" (Washington: 2022), available at https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.

17 Consumer Financial Protection Bureau, "CFPB and Federal Partners Confirm Automated Systems and Advanced Technology Not an Excuse for Lawbreaking Behavior," Press release, April 25, 2023, available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-federal-partners-confirm-automated-systems-advanced-technology-not-an-excuse-for-lawbreaking-behavior/.

18 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

19 Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?"

20 NIST Computer Security Resource Center, "Red Team/Blue Team Approach," available at https://csrc.nist.gov/glossary/term/red_team_blue_team_approach (last accessed May 2024).

21 Simon Toms and others, "How Regulators Worldwide Are Addressing the Adoption of AI in Financial Services," Skadden, December 12, 2023, available at https://www.skadden.com/insights/publications/2023/12/how-regulators-worldwide-are-addressing-the-adoption-of-ai-in-financial-services; Board of Governors of the Federal Reserve System and others, "Agencies seek wide range of views on financial institutions' use of artificial intelligence."

22 U.S. Bank, "How AI in treasury management is transforming finance," May 19, 2023, available at https://www.usbank.com/financialiq/improve-your-operations/manage-payments/ai-thinks-treasury-management-is-ready-for-transformation.html.

23 Miriam Fernández, "AI in Banking: AI Will Be An Incremental Game Changer," S&P Global, October 31, 2023, available at https://www.spglobal.com/en/research-insights/featured/special-editorial/ai-in-banking-ai-will-be-an-incremental-game-changer.

24 Legal Information Institute, "Definition: systemic importance from 12 USC § 5462(9)," available at https://www.law.cornell.edu/definitions/uscode.php?height=800&def_id=12-USC-1184801643-149939311&term_occur=999&term_src=title:12:chapter:53:subchapter:IV:section:5463 (last accessed February 2024).

25 Emil Sayegh, "Artificial Intelligence and Clouds: A Complex Relationship of Collaboration and Concern," Forbes, August 23, 2023, available at https://www.forbes.com/sites/emilsayegh/2023/08/23/artificial-intelligence-and-clouds-a-complex-relationship-of-collaboration-and-concern/?sh=217106475c19.

26 Pete Schroeder, "U.S. House lawmakers ask regulators to scrutinize bank cloud providers," Reuters, August 23, 2019, available at https://www.reuters.com/article/us-usa-congress-cloud-idUSKCN1VD0Y4/; Action Center on Race & the Economy and others, "Letter to Members of the Financial Stability Oversight Council," November 23, 2021, available at https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/619ce27890a0062ae7014dfd/1637671544609/Designate+AWS+as+a+Systemically+Important+Financial+Market+Utility.pdf.

27 Legal Information Institute, "17 CFR § 240.15c3-1e - Deductions for market and credit risk for certain brokers or dealers (Appendix E to 17 CFR 240.15c3-1)," available at https://www.law.cornell.edu/cfr/text/17/240.15c3-1e (last accessed May 2024).

28 Jay Clayton, "Regulation Best Interest and the Investment Adviser Fiduciary Duty: Two Strong Standards that Protect and Provide Choice for Main Street Investors," U.S. Securities and Exchange Commission, July 8, 2019, available at https://www.sec.gov/news/speech/clayton-regulation-best-interest-investment-adviser-fiduciary-duty.

29 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

30 Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?"

31 Mohar Chatterjee, "AI might have already set the stage for the next tech monopoly," Politico, March 22, 2023, available at https://www.politico.com/newsletters/digital-future-daily/2023/03/22/ai-might-have-already-set-the-stage-for-the-next-tech-monopoly-00088382.

32 Ibid.

33 Executive Office of the President, "Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

34 Siddiqui, "Red Teams vs. Blue Teams: What's The Difference?"

35 Chatterjee, "AI might have already set the stage for the next tech monopoly."