epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Office of Science and Technology Policy

on

Request for Information on National Priorities for Artificial Intelligence

July 7, 2023

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Office of Science and Technology Policy (OSTP)'s recent request for information regarding its National Artificial Intelligence (AI) Strategy.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus on public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[1] EPIC has a long history of promoting transparency and accountability for information technology.[2]

EPIC commends the OSTP for its fantastic work developing and rolling out the *Blueprint for an AI Bill of Rights* and urges the agency to carry the Blueprint forward when developing the Administration's AI strategy. In these comments, EPIC identifies key elements of existing federal AI frameworks that should be incorporated into the National AI Strategy; advises the federal government to lead by example as a user, funder, and evaluator of AI systems; calls on the OSTP in particular to develop sector-specific guidance for (and in collaboration with) agencies that regulate the use of AI in the private sector; and urges the federal government to center risks, rights, and responsibilities in its approach to AI rather than prioritizing aggressive adoption of automated decision-making technologies.

Both the OSTP and the National Institute of Standards and Technology (NIST) have thought carefully about responsible development and use of AI. As you know, both agencies have published recommendations for creators, purchasers, and users of AI systems and have laid out rights and

[1] EPIC, *About Us* (2023), https://epic.org/about/.

[2] *See, e.g.*, EPIC, *AI & Human Rights* (2023), https://epic.org/issues/ai/; EPIC, *AI in the Criminal Justice System* (2023), https://epic.org/issues/ai/ai-in-the-criminal-justice-system/; EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* (2023), https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf [hereinafter "EPIC Generating Harms Report"]; EPIC, *Screened & Scored in the District of Columbia* (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf [hereinafter "EPIC Screened & Scored Report"]; Comments of EPIC, *In re Privacy, Equity, and Civil Rights Request for Comment* (Mar. 6, 2023), https://epic.org/wp-content/uploads/2023/03/EPIC-comments-NTIA-DiversityEquityCivilRights-RFC.pdf.

expectations that individuals are entitled to with respect to AI. EPIC recommends that the OSTP incorporate essential elements from both documents.

From the OSTP's *Blueprint for an AI Bill of Rights*,[3] we highlight in particular:

- "Independent evaluation and plain language reporting in the form of an algorithmic impact assessment, including disparity testing results and mitigation information, should be performed and made public whenever possible to confirm these protections."[4]
- "You should be protected from violations of privacy through design choices that ensure such protections are included by default, including ensuring that data collection conforms to reasonable expectations and that only data strictly necessary for the specific context is collected."[5]
- "Systems should undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards."[6]
- "Independent evaluation and reporting that confirms that the system is safe and effective, including reporting of steps taken to mitigate potential harms, should be performed and the results made public whenever possible."[7]
- "Surveillance or monitoring systems should be subject to heightened oversight that includes at a minimum assessment of potential harms during design (before deployment) and in an ongoing manner, to ensure that the American public's rights, opportunities, and access are protected. This assessment should be done before deployment and should give special attention to ensure there is not algorithmic discrimination[.] Such assessment should then be reaffirmed in an ongoing manner as long as the system is in use."[8]
- "You should know how and why an outcome impacting you was determined by an automated system, including when the automated system is not the sole input determining the outcome."[9]
- "Automated systems should provide explanations that are technically valid, meaningful and useful to you and to any operators or others who need to understand the system and calibrated to the level of risk based on the context."[10]

Similarly, EPIC wishes to highlight the following assurance mechanisms from NIST's *Artificial Intelligence Risk Management Framework* and *AI RMF Playbook*:

[3] OSTP, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[4] *Id.* at 23.

[5] *Id.* at 30.

[6] *Id.* at 15.

[7] *Id.*

[8] *Id.* at 15.

[9] *Id.* at 34.

[10] *Id.* at 40.

- Identify AI actors responsible for evaluating efficacy of risk management processes and approaches, and for course-correction based on results.[11]
- Establish and regularly review documentation policies that, among others, address information related to: (1) AI actors contact information; (2) business justification; (3) scope and usages; (4) assumptions and limitations; (5) description and characterization of training data; (6) algorithmic methodology; (7) evaluated alternative approaches; (8) description of output data; (9) testing and validation results (including explanatory visualizations and information); (10) down- and up-stream dependencies; (11) plans for deployment, monitoring, and change management; and (12) stakeholder engagement plans.[12]
- Establish policies that promote effective challenges of AI system design, implementation, and deployment decisions, via mechanisms such as the three lines of defense, model audits, or red-teaming – to ensure that workplace risks such as groupthink do not take hold.[13]
- Establish policies that incentivize safety-first mindset and general critical thinking and review at an organizational and procedural level.[14]
- Establish whistleblower protections for insiders who report on perceived serious problems with AI systems.[15]
- Establish impact assessment policies and processes for AI systems used by the organization.[16]
- Verify that impact assessment activities are appropriate to evaluate the potential negative impact of a system and how quickly a system changes, and that assessments are applied on a regular basis.[17]
- Utilize impact assessments to inform broader evaluations of AI system risk.[18]
- Respond to and document detected or reported negative impacts or issues in AI system performance and trustworthiness.[19]
- Document the basis for decisions made relative to tradeoffs between trustworthy characteristics, system risks, and system opportunities.[20]
- Maintain a database of reported errors, incidents and negative impacts including date reported, number of reports, assessment of impact and severity, and responses.[21]
- Maintain a database of system changes, reason for change, and details of how the change was made, tested, and deployed.[22]
- Utilize TEVV (Test, Evaluation, Verification, Validation) outputs from map and measure functions when considering risk treatment.[23]

[11] NIST, *NIST AI Risk Management Framework Playbook – Govern* 7 (Jan. 28, 2023), https://github.com/usnistgov/AIRMF/blob/nist-pages/govern/govern.pdf.
[12] *Id.* at 6.
[13] *Id.* at 18.
[14] *Id.*
[15] *Id.* at 4, 18.
[16] *Id.* at 19.
[17] *Id.*
[18] *Id.*
[19] NIST, *NIST AI Risk Management Framework Playbook – Manage* 17 (Jan. 28, 2023), https://github.com/usnistgov/AIRMF/blob/nist-pages/manage/manage.pdf.
[20] *Id.* at 18.
[21] *Id.* at 19.
[22] *Id.*
[23] *Id.* at 2.

- Establish mechanisms to capture feedback from system end users and potentially impacted groups.[24]
- Establish risk controls considering trustworthiness characteristics, including: (1) data management, quality, and privacy (e.g., minimization, rectification, or deletion requests) controls as part of organizational data governance policies; (2) machine learning and end-point security countermeasures (e.g., robust models, differential privacy, authentication, throttling); (3) business rules that augment, limit or restrict AI system outputs within certain contexts; (4) utilizing domain expertise related to deployment context for continuous improvement and TEVV across the AI lifecycle; (5) development and regular tracking of human-AI teaming configurations; (6) model assessment and test, evaluation, validation and verification (TEVV) protocols; (7) use of standardized documentation and transparency mechanisms; (8) software quality assurance practices across AI lifecycle; and (9) mechanisms to explore system limitations and avoid past failed designs or deployments.[25]
- Establish and maintain procedures to regularly monitor system components for drift, decontextualization, or other AI system behavior factors.[26]
- Establish and maintain procedures for capturing feedback about negative impacts.
- Evaluate AI system trustworthiness in conditions similar to deployment context of use, and prior to deployment.[27]
- Regularly assess and document system performance relative to trustworthiness characteristics and tradeoffs between negative risks and opportunities.[28]
- Evaluate AI system oversight practices for validity and reliability. When oversight practices undergo extensive updates or adaptations, retest, evaluate results, and course correct as necessary.[29]
- Review audit reports, testing results, product roadmaps, warranties, terms of service, end user license agreements, contracts, and other documentation related to third-party entities to assist in value assessment and risk management activities.[30]
- Track third parties preventing or hampering risk-mapping as indications of increased risk.[31]
- Review third-party material (including data and models) for risks related to bias, data privacy, and security vulnerabilities.[32]
- Establish assessment scales for measuring AI systems' impact. Scales may be qualitative, such as red-amber-green (RAG) or may entail simulations or econometric approaches. Document and apply scales uniformly across the organization's AI portfolio.[33]
- Apply TEVV regularly at key stages in the AI lifecycle, connected to system impacts and frequency of system updates.[34]

[24] *Id.* at 8.
[25] *Id.*
[26] *Id.* at 12.
[27] *Id.* at 17.
[28] *Id.* at 2.
[29] NIST, *NIST AI Risk Management Framework Playbook – Map* 22 (Jan. 28, 2023), https://github.com/usnistgov/AIRMF/blob/nist-pages/map/map.pdf.
[30] *Id.* at 24.
[31] *Id.* at 25.
[32] *Id.*
[33] *Id.* at 27.
[34] *Id.*

- Develop TEVV procedures that incorporate socio-technical elements and methods and plan to normalize across organizational culture.[35]
- Regularly review and refine TEVV processes.[36]
- Apply traditional technology risk controls—such as procurement, security, and data privacy controls—to all acquired third-party technologies.[37]

I. Lead by Example

The federal government plays a major role in today's AI economy, and EPIC urges the OSTP and the Biden-Harris Administration to lead by example when it develops, procures, and uses AI. Demonstrating responsible AI design, development, procurement, and use will help both government agencies and private AI actors put frameworks like the Blueprint for an AI Bill of Rights and NIST's AI Risk Management Framework into practice. EPIC will follow up with your office in the coming months with more specific input on the role of government within the AI economy, but agencies must lead in their role as *users and purchasers* of technology from vendors; as *funders* of state and local agencies and researchers that apply federal grants toward AI systems; and as *independent, rights-focused evaluators* of AI systems.

As User: The federal government uses automated decision-making tools but authoritative information about these systems is often unavailable to the public. Despite numerous executive orders, efforts by the Administrative Conference on the United States, public records requests, and Congressional oversight, federal use of and spending on AI systems remains significant but deeply opaque. Moreover, federal agencies routinely fail to evaluate the bias, privacy, and operational impacts of the AI tools they develop and deploy. The use case inventories required several years ago under EO 13,960 were supposed to shed light on federal AI use but is incomplete.[38]

This lack of transparency and accountability in federal AI adoption presents significant risks to the public. Unreasonable overreliance on AI and automated decision-making systems incentivizes increased sensitive data collection; risks dehumanizing constituents; and threatens the legitimacy of the administrative state itself.[39]

To help prevent this, OSTP should establish a user-friendly portal disclosing the details of each AI system that federal agencies are developing, purchasing, using, or considering for adoption. This database could be incorporated into AI.gov, which has become a helpful resource for researchers, civil society, and the public. At a minimum, this portal should disclose for each system:

- The intended use of system and reasonably foreseeable uses outside of that intended use;
- The carbon footprint of the development and ongoing use of the system;

[35] *Id.* at 28.
[36] *Id.*
[37] *Id.* at 25.
[38] Ben Winters, *Two Key AI Transparency Measures from Executive Orders Remain Largely Unfulfilled Past Deadlines*, EPIC Blog (Jan. 26, 2022), https://epic.org/unfulfilled-ai-executive-orders/; National Artificial Intelligence Initiative Office, *Agency Inventories of AI Use Cases* (last visited Jul. 7, 2023), https://www.ai.gov/ai-use-case-inventories/.
[39] Ryan Calo & Danielle K. Citron, *The Automated Administrative State: A Crisis of* Legitimacy, 70 Emory L. J. 797 (2021), https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj.

- An assessment of the relative benefits and costs to the public given the system's purpose, capabilities, and probable use cases;
- The inputs and logic of the system;
- Detailed use and data management policies, including how the data relied on by the system is collected, processed, secured, and timely disposed of;
- The type(s) of outputs the system generates;
- Whether the outputs could be used downstream for any purpose not previously articulated; and
- Yearly validation studies.

As Funder: Federal agencies play a massive role in funding AI development. There are direct funding impacts from agencies procuring specific tools, and less direct funding choices in how to implement programs like the National AI Research Resource. Research funding priorities must change toward evaluation, safety, and determining when the use of an automated tool is appropriate.

In response to a 2021 request by Senator Ron Wyden, the Department of Justice made a troubling disclosure: the DOJ itself had no records about which grants awarded by the Department were used to buy predictive policing.[40] Predictive policing algorithms have a disparate impact on people of color because they are built on "dirty data" that recreates historically biased law enforcement practices.[10] As of 2021 based on publicly available information, the Department of Justice has awarded over $57,000,000 in grants to local police departments through Smart Policing Programs.[41] Since 2021, the DOJ has granted $3,943,002 to police departments to improve "data-driven" policing, "smart" policing, and related activities.[42] The Pasco County Sherriff's predictive policing tool, which was created with federal funds, was used to "monitor and harass families across the country," even when police acknowledged that the subjects of this harassment had not violated the law but were merely predicted to do so in the future.[43] Federal agencies must provide funding responsibly and methodically, setting a high standard for the systems that can be used with federal dollars, ensuring that it complies with Title VI of the Civil Rights Act.

As Evaluator: The federal government is uniquely equipped to provide desperately needed algorithmic evaluation talent and capacity. Considerable federal funding has been committed to the study, support, and development of AI tools, even including helpful evaluation frameworks and principles. However, the U.S. must move past this, allocating resources to training and hiring individuals with algorithmic auditing expertise. This could be done in a variety of ways. One proposal is for the Federal CIO Council and NIST to partner to train, place, and manage evaluators through a similar model to the Presidential Innovation Fellowships. The rubrics of evaluation can be developed using NIST's AI RMF working with the CIO Council to ensure government agencies could feasibly achieve consistent evaluation. In addition to being able to evaluate *internal* use, agencies must be equipped to evaluate private uses for investigation and enforcement.

[40] Dell Cameron, *Justice Department Admits: We Don't Even Know How Many Predictive Policing Tools We've Funded*, Gizmodo (Mar. 17, 2022), https://gizmodo.com/justice-department-kept-few-records-on-predictive-polic-1848660323.

[41] *Funding & Awards*, Bureau Just. Assistance (2022), https://bja.ojp.gov/funding.

[42] *Id*.

[43] Kathleen McGrory & Neil Bedi, *Targeted*, Tampa Bay Times (Sept. 3, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing.

II. Guide Agencies to Regulate

The OSTP should instruct agencies to use their investigatory powers to elucidate how automated systems are used in the industries they regulate, monitor, or participate in. In these reports, agencies should publish clear, public tables that illustrate the types of technologies used in the sectors they regulate, including examples. These resources should be made public in line with compliance with the transparency measures in Executive Orders 13859 and 13960 and should not exempt law enforcement agencies or AI applications.[44]

The OSTP should also distribute sector-specific advice on algorithmic bias concerns and work with enforcement agencies to close knowledge gaps concerning the risks of AI.

III. Center Risks and Responsibility in AI Oversight

In addition to its general comments around responsible AI development, procurement, oversight, and use, EPIC offers the following responses to specific questions posed within the OSTP's Request for Information:

A. Responsible AI Development Requires Careful Review of the Externalized Risks that AI Development Imposes on the Public, the Economy, the Climate, and the Government.

The following is responsive to Questions 7, 8, 10, 15, 20, and 21.

AI innovation, like all technological innovation, risks producing harm in addition to economic growth.[45] However, the harms of AI innovation—harms to marginalized populations, competition, the climate, and democratic processes, for example[46]—are often difficult to calculate.[47] In practice, this means that efforts to spur responsible AI innovation may be distorted in favor of calculable, economic benefits (often flowing toward private AI developers) over incalculable, externalized harms (often impacting vulnerable populations). The OSTP's Request for Information therefore comes at a critical juncture for AI oversight: effective AI regulation and oversight can still correct the course of AI innovation and ensure AI technologies benefit the public moving forward.

The first step to responsible AI development is clearly articulating the scope and variety of AI risks—risks that may be ignored or externalized by private AI developers.[48] Luckily, even as AI technologies continue to advance, many of their risks remain the same.[49] These risks include, but are not limited to: (1) risks involving information manipulation and the spread of misinformation; (2)

[44] Winters, *supra* note 38.

[45] *See, e.g.*, EPIC Generating Harms Report; Daron Acemoglu, *Harms of AI* 10 (Nat'l Bureau of Econ. Rsch., Working Paper No. 29247, 2021), https://www.nber.org/system/files/working_papers/w29247/w29247.pdf; Ulrich Witt, *Innovations, Externalities and the Problem of Economic Progress*, 89 Pub. Choice 113 (1996).

[46] *See* EPIC Generating Harms Report.

[47] *See* Witt, *supra* note 45.

[48] *See, e.g.*, Timnit Gebru et al., *Statement from the Listed Authors of Stochastic Parrots on the "AI Pause" Letter*, DAIR (Mar. 31, 2023), https://www.dair-institute.org/blog/letter-statement-March2023/.

[49] For years, AI scholars and ethicists have warned that AI technologies impose serious, societal risks. *See, e.g.*, Emily M. Bender et al., *On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?*, Proc. 2021 ACM Conf. on Fairness, Accountability, & Transparency 610 (2021); Vinodkumar Prabhakaran et al., *A Human Rights-Based Approach to Responsible AI*, arXiv (Oct. 6, 2022), https://arxiv.org/pdf/2210.02667.pdf.

risks of harassment, impersonation, fraud, or extortion; (3) risks of privacy violations involving increasingly opaque data collection and use; (4) data security risks; (5) risks to creative industries due to the impact of AI on intellectual property rights; (6) risks that AI technologies will exacerbate the effects of climate change; (7) risks involving labor manipulation, theft, and displacement; (8) various risks involving AI discrimination; and (8) risks to competition within various markets impacted by AI.[50] Rather than discuss each AI risk in detail within this comment, EPIC refers the OSTP to our recent report, *Generating Harms: Generative AI's Impact & Paths Forward*, available at epic.org/GAI. Although the report focuses on generative AI technologies, the myriad risks analyzed therein apply to other AI technologies as well.

When weighing the benefits of AI technologies against their risks, EPIC urges the OSTP and the National AI Strategy to carefully evaluate not only the calculable benefits and risks of AI technologies, but also the incalculable and disparate risks that AI systems pose to vulnerable groups, the climate, and democratic processes. Only after these non-economic risks are identified and mitigated can AI design, development, and deployment be truly responsible.

B. Regulatory Obligations and Examples of Responsible AI Design, Development, and Deployment are Necessary for a Successful AI Oversight Framework

The following is responsive to Questions 1-3, 12, and 13.

OSTP's Blueprint for an AI Bill of Rights and NIST's AI Risk Management Framework provide a valuable foundation for responsible AI design, development, and deployment, but voluntary frameworks are not sufficient, by themselves, to ensure that AI systems are designed, developed, and deployed responsibly.[51] Entities developing and using AI systems need *regulatory obligations* and *specific guidance* on what actions will impose costs, regulatory scrutiny, or legal liability in order for any responsible AI frameworks to be effective.[52] If the first step to responsible AI development and use is identifying and prioritizing AI risks to the public, democracy, and the environment, implementing regulatory obligations and specific guidance is the second step.

Regulatory Obligations: Private companies developing and deploying AI technologies are incentivized to innovate in ways that boost their profits and market power, often in ways that can harm the public. For example, when large technology companies like Google and Microsoft began racing to incorporate generative AI models into their service offerings earlier this year, their rollout produced serious, widespread harms to the public and the environment, including privacy violations,[53] consumer harms,[54] violations to intellectual property rights,[55] and environmental

[50] EPIC Generating Harms Report.

[51] *See* EPIC Comments on the FTC's Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 84–86, R111004 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter "EPIC FTC Commercial Surveillance Comments"]; *cf. generally* Luke Munn, *The Uselessness of AI Ethics*, AI and Ethics, Aug 2022.

[52] *See* EPIC FTC Commercial Surveillance Comments at 84–86.

[53] *See* Tonya Riley, *OpenAI Lawsuit Reignites Privacy Debate Over Data Scraping*, Cyberscoop (June 30, 2023), https://cyberscoop.com/openai-lawsuit-privacy-data-scraping/.

[54] *See* Michael Atleson, *The Luring Test: AI and the Engineering of Consumer Trust*, FTC Business Blog (May 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust.

[55] *See* Christopher T. Zirpoli, Cong. Rsch. Serv., LSB10922, Generative Artificial Intelligence and Copyright Law (2023), https://crsreports.congress.gov/product/pdf/LSB/LSB10922.

harms.[56] To counteract these incentives, mandatory oversight mechanisms are needed. These mechanisms include but are not limited to: (1) minimum AI model testing and evaluation, (2) regular AI impact assessments, (3) AI transparency requirements, and (4) data sourcing and use restrictions. Above all, AI systems need to be *provably* accurate, effective, and unbiased both before and during deployment, and AI systems that fail to meet minimum accuracy, safety, and nondiscrimination standards must be prohibited. Only mandatory testing and reporting obligations can *ensure* that private companies develop and deploy AI responsibly.

Mandatory testing and reporting obligations can also improve government development and use of AI—and there may be a sufficient statutory basis for imposing these obligations on federal agencies today. Under Section 208 of the E-Government Act of 2002,[57] federal agencies are required to complete privacy impact assessments (PIAs) before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form."[58] These PIAs must include, *inter alia*, what information the agency will collect, the purpose of collection, how the agency will use the information, and with whom the information will be shared.[59] Crucially, because AI technologies require the collection and use of information—often including sensitive personal information—to operate, Section 208 of the E-Government Act can be interpreted to require federal agencies to complete a PIA when they develop or procure an AI system. Further, because agencies are required to follow the PIA guidance issued by the Office of Management and Budget (OMB) under Section 208,[60] the Biden-Harris Administration could impose AI impact assessments, audits, or other testing and reporting obligations on federal agencies by directing the OMB to include responsible AI measures within its PIA guidance. EPIC will provide the OSTP with more detail on this proposal in the near future.

Specific Guidance: In addition to mandatory obligations, specific federal guidance can help companies conform to responsible AI requirements by reducing the costs (and guesswork) that companies face when attempting to improve their AI development practices. As discussed above, AI companies may want to comply with responsible AI guidelines but do not know what is required. By modeling compliant and responsible behavior within federal government and providing guidance on what specific acts or practices constitute responsible AI development, the OSTP can incentivize industry compliance by reducing the costs of voluntary compliance.

Together, regulatory obligations and specific AI guidance create an enforceable, minimum standard for responsible AI design, development, and deployment. These measures should be implemented, at least in part, by federal agencies capable of enforcing responsible AI obligations within the private sector, including the Department of Justice, the Federal Trade Commission, and the Consumer Financial Protection Bureau. However, the OSTP can play a key role in both articulating and standardizing what responsible AI standards and enforcement could look like.

[56] *See* Akielly Hu, *AI is Hurting the Climate in a Number of Non-Obvious Ways*, Markup (July 6, 2023), https://themarkup.org/news/2023/07/06/ai-is-hurting-the-climate-in-a-number-of-non-obvious-ways.
[57] 44 U.S.C. § 3501 note.
[58] *Id.*
[59] *Id.*
[60] Throughout Section 208, the term, "shall," is repeatedly used instead of more permissive terms like "may." *Id.*

C. Federal Funding and Procurement Guidelines May Also Mitigate the Risks and Harms of Government AI Use.

The following is responsive to Questions 26-28.

In addition to direct AI oversight, the Biden-Harris Administration can promote more responsible AI development and use indirectly through federal funding and procurement guidance. Today, many AI systems are developed and deployed for use by state and federal agencies—and the market is lucrative. As of June 2023, the Department of Labor has made available $1.6 billion in American Rescue Plan Act (ARPA) funds to help states modernize their IT systems and prevent identity fraud;[61] much of these funds are spent procuring and maintaining AI systems.[62]

Given the extent of federal funding directed toward state modernization efforts and other AI-related purposes, the Biden-Harris Administration should restrict how and when federal funding can be used to procure and maintain AI systems both within federal government and through federally funded state programs. These restrictions may include but are not limited to: (1) requiring AI vendors to provide regular AI audits and impact assessments; (2) requiring AI vendors and agencies to follow certain AI transparency, data-sourcing, or responsible use obligations before they receive federal money; and (3) directing federal investment into AI oversight efforts such that agencies can adopt and maintain responsible AI oversight processes.

IV. Conclusion

EPIC applauds the OSTP for leading the administration interest in prioritizing rights in the age of AI. If you have any questions, we remain available and eager to answer any questions.

Respectfully submitted,

/s/ *Ben Winters*	/s/ *Grant Fergusson*
Ben Winters	Grant Fergusson
Senior Counsel	Equal Justice Works Fellow

Referenced:

EPIC's *Generating Harms* Report, which can be found at epic.org/GAI.

[61] Press Release, U.S. Dep't of Labor, US Department of Labor Announces Up to $200M in Available Grants to States to Strengthen Unemployment Insurance Programs; Prevent, Detect Fraud (Apr. 27, 2023), https://www.dol.gov/newsroom/releases/eta/eta20230427-0.

[62] *See* Grant Fergusson, *Public Benefits, Private Vendors: How Private Companies Help Run Our Welfare Programs*, EPIC Blog (Jan. 26, 2023), https://epic.org/public-benefits-private-vendors-how-private-companies-help-run-our-welfare-programs/; *cf.* EPIC Screened and Scored Report.