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 MANAGEMENT AND BUDGET

Request for Comments on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum

No. 2023-24269

December 5, 2023

TABLE OF CONTENTS

INTRODUCTION

The Electronic Privacy Information (EPIC) submits these comments in response to the Office of Management and Budget (OMB)'s Request for Comments on its "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" Draft Memorandum, published on November 3, 2023.[1]

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] We advocate for a human-rights based approach to AI policy that ensures new technologies are subject to democratic governance.[3] Over the last decade, EPIC has consistently advocated for the adoption of clear, commonsense, and actionable AI regulations across the country.[4] EPIC has litigated cases against the U.S. Department of Justice to compel production of documents regarding "evidence-based risk assessment tools"[5], against the U.S. Department of Homeland Security to produce documents about a program purported to assess the probability that an individual will commit a crime,[6] and against the National Security Commission on Artificial Intelligence (NSCAI) to enforce its transparency obligations under the Freedom of Information Act and the Federal Advisory Committee Act.[7] EPIC has also published extensive research on

[1] Request for Comments on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum, 88 Fed. Reg. 75625 (Nov. 3, 2023).
[2] *About Us*, EPIC, https://epic.org/about/ (2023).
[3] *See, e.g.*, *AI and Human Rights*, EPIC, https://epic.org/issues/ai/ (2023); *AI and Human Rights: Criminal Legal System*, EPIC, https://epic.org/issues/ai/ai-in-the-criminal-justice-system/ (2023); EPIC, Outsourced & Automated: How AI Companies Have Taken Over Government Decision-Making (2023), https://epic.org/outsourced-automated/ [hereinafter "Outsourced & Automated Report"]; Letter from EPIC to President Biden and Vice President Harris on Ensuring Adequate Federal Workforce and Resources for Effective AI Oversight (Oct. 24, 2023), https://epic.org/wp-content/uploads/2023/10/EPIC-letter-to-White-House-re-AI-workforce-and-resources-Oct-2023.pdf; EPIC, Comments on the NIST Artificial Intelligence Risk Management Framework: Second Draft (Sept. 28, 2022), https://epic.org/wp-content/uploads/2022/09/EPIC-Comments-NIST-RMF-09-28-22.pdf.
[4] *See, e.g.*, Press Release, EPIC, EPIC Urges DC Council to Pass Algorithmic Discrimination Bill (Sept. 23, 2022), https://epic.org/epic-urges-dc-council-to-pass-algorithmic-discrimination-bill/; EPIC, Comments to the Patent and Trademark Office on Intellectual Property Protection for Artificial Intelligence Innovation (Jan. 10, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-USPTO-Jan2020.pdf; EPIC, Comments on the Department of Housing and Urban Development's Implementation of the Fair Housing Act's Disparate Impact Standard (Oct. 18, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-HUD-Oct2019.pdf.
[5] *EPIC v. DOJ*, 320 F. Supp. 3d 110 (D.D.C. 2018), *voluntarily dismissed,* 2020 WL 1919646 (D.C. Cir. 2020), https://epic.org/foia/doj/criminal-justice-algorithms/.
[6] *See EPIC v. DHS – FAST Program*, EPIC, https://epic.org/documents/epic-v-dhs-fast-program/ (last visited Dec. 5, 2023).
[7] *EPIC v. NSCAI*, 419 F. Supp. 3d 82, 86, 95 (D.D.C. 2019), https://epic.org/documents/epic-v-ai-commission/.

emerging AI technologies like generative AI,[8] as well as the ways that government agencies develop, procure, and use AI systems around the country.[9]

At all levels of government, administrative agencies are granted authority to exercise a wide array of enforcement, adjudicative, and rulemaking powers due to their unique expertise—and agencies' reliance on AI systems when exercising these powers can erode the accuracy, reliability, and legitimacy of government decisions.[10] Government AI systems can undermine individuals' control over their data and fortify the position of data-extractive technologies and data brokers.[11] They can perpetuate and obscure inaccuracies and bias within data in ways that undermine individuals' civil rights and access to government services.[12] And without sufficient transparency and oversight, government AI systems can undermine decades-old processes for ensuring that government agencies meet their legal and regulatory obligations.[13]

RECOMMENDATION

EPIC submits these comments to **(1)** express support for OMB's inclusion of several key responsible AI provisions that will rebuff many risks imposed by government AI uses, including but not limited to AI impact assessments, a publicly available AI use case inventory, and AI-specific procurement processes; **(2)** recommend additional refinements to these responsible AI provisions, including additional refinements for AI impact assessments and AI use case inventories; **(3)** urge OMB to encourage AI adoption only where AI can serve as a curated tool to meet predefined agency needs; **(4)** caution OMB against implementing the Draft Memorandum without mechanisms to ensure agency compliance; and **(5)** urge OMB to narrowly construe national security system exclusions throughout the Draft Memorandum.

[8] EPIC, Generating Harms: Generative AI's Impact & Paths Forward (2023), https://epic.org/gai [hereinafter "EPIC Generative AI Report"].

[9] Outsourced & Automated 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 "Screened & Scored Report"].

[10] *See* Outsourced & Automated Report at 6–25; Ryan Calo & Danielle Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 Emory L.J. 797, 799–800 (2021).

[11] Outsourced & Automated Report at 12; *see also* Danielle Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793, 845–55 (2022).

[12] Outsourced & Automated Report at 17–20; *see also* Screened & Scored Report at 17, 19–21; Mary Flanagan et al., *Embodying Values in Technology: Theory and Practice*, *in* Information Technology and Moral Philosophy 322, 322–47 (Jeroen van den Hoven & John Weckert eds., 2008).

[13] *See* Outsourced & Automated Report at 21–25; Calo & Citron, *supra* note 10, at 799–800; Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 Berkeley Tech. L.J. 781, 787–88 (2019).

I. Key Aspects of OMB's Draft Memorandum Can and Should be Fortified

Safety-Impacting and Rights-Impacting AI Designations

Responsive to Questions 5-7

EPIC applauds OMB's adoption of comprehensive risk designations and minimum risk managements practices required for agencies using any AI system deemed safety-impacting or rights-impacting. Ensuring that agencies maintain both pre-deployment and ongoing testing, evaluation, and risk management processes is foundational for any responsible AI paradigm. In particular, EPIC applauds the inclusion of (1) pre-deployment impact assessments to identify intended uses, risks, limitations, and data misuse or overuse and ongoing; (2) ongoing and independent AI testing to ensure federal AI systems are accurate, reliable, and unbiased; (3) human training and assessment provisions to ensure agency employees have the skills and resources they need to adequately oversee AI development, procurement, and use; (4) public, plain-language notice of AI use to ensure the public is aware of how their government is using AI; (5) requirements to involve—and inform—affected groups when a federal AI systems may impact them; and (6) a provision requiring convenient opt-outs in favor of human alternatives. Many government AI systems are still prone to serious errors and biases,[14] and these minimum safety requirements are a strong mechanism for mitigating AI harms and maintaining accountability for agency use of AI technologies.

In part because OMB's suggested minimum practices are robust, EPIC fears that agencies and AI contractors may seek to circumvent OMB's minimum practices altogether either by determining that edge-case AI applications fall outside the scope of OMB's safety-impacting and rights-impacting AI designations or by liberally granting waivers to the minimum practices. The challenge of determining whether edge-case AI applications should receive greater evaluation and oversight is not new. In Europe, for example, regulators drafting the European Union's AI Act have struggled to draw clean lines between risk designations for newer and emerging AI technologies like foundational models.[15] And while the European Commission has more recently

[14] *See, e.g.*, Outsourced & Automated Report at 5–25.

[15] *See, e.g.*, Will Henshall, *E.U.'s AI Regulation Could be Softened After Pushback from Biggest Members*, Time (Nov. 22, 2023), https://time.com/6338602/eu-ai-regulation-foundation-models/ ("Big tech companies, largely headquartered in the U.S., have been lobbying to weaken the proposed E.U. legislation throughout its development."); Supantha Mukherjee & Foo Yun Chee, *EU Lawmakers Face Struggle to Reach Agreement on AI Rules—Sources*, Reuters (Oct. 23, 2023), https://www.reuters.com/technology/eu-lawmakers-face-struggle-reach-agreement-ai-rules-sources-2023-10-23/; Billy Perrigo, *Big Tech is Already Lobbying to Water Down Europe's AI Rules*, Time (Apr. 21, 2023), https://time.com/6273694/ai-regulation-europe/.

suggested moving toward light touch "codes of practice,"[16] such a compromise position will *not* ensure that AI systems are accurate, reliable, trustworthy, or responsibly deployed.

Similarly, consider edge-case AI applications like automated notice generation systems.[17] While OMB's Draft Memorandum presumes that AI decisions about, e.g., someone's eligibility for public benefits or loans are rights-impacting, it is currently silent on automated systems used to notify applicants of outstanding documents, process expectations, eligibility determinations, or options for appeal. These automated notice generation systems may not directly influence the outcome of a decision-making process, but any errors they produce *can* hinder an applicant during the decision-making process: delays in notice delivery, errors in the substance of the notice, and the failure to generate notices can all undermine an applicant's ability to provide proper documentation, respond to questions, and pursue timely appeals. Faced with robust minimum practices for safety-impacting and rights-impacting AI systems and no required AI practices for AI systems deemed outside the scope of either designation, agencies and contractors will be incentivized to circumvent the Draft Memorandum's risk practices through narrow interpretations of risk designations and waivers.

To mitigate the risk that harmful AI use cases and agency practices evade proper scrutiny under the Draft Memorandum, **EPIC proposes four recommendations**:

1. OMB should require agencies to incorporate certain **minimum risk practices for *all* federal AI use cases**, such as ensuring adequate human training and completing a rudimentary AI impact assessment when determining whether an AI system is safety-impacting or rights-impacting.

2. OMB should **explicitly prohibit or deem presumptively noncompliant AI use cases that are provably harmful or biased**, including emotion recognition, biometric categorization, social scoring, and one-to-many facial recognition.

3. OMB should incorporate **explicit principles of data minimization** into federal AI development, procurement, and use standards.

4. OMB should include **additional protections for sensitive personal data**—protections that may include a **strict necessity data minimization** standard.

RECOMMENDATION

[16] *See* Luca Bertuzzi, *AI Act: EU Commission Attempts to Revive Tiered Approach Shifting to General Purpose AI*, Euractiv (Nov. 20, 2023), https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-commission-attempts-to-revive-tiered-approach-shifting-to-general-purpose-ai/.
[17] *Cf.* Outsourced & Automated Report at 11, 35.

a. Recommendation One: Expand Minimum Practices and Oversight

OMB should require agencies to incorporate certain minimum risk practices for *all* federal AI use cases—and implement an independent oversight process for determinations concerning safety-impacting and rights-impacting designations. Universally applicable AI risk management practices and independent AI designations would ensure that the agencies tasked with evaluating AI applications and mitigating AI risks do not cut corners by trying to circumvent the risk management process altogether. In addition, universally applicable AI risk management practices would ensure that AI vendors could not creatively market their products to avoid proper scrutiny.[18]

Several minimum practices already outlined within OMB's Draft Memorandum would be feasible as universally applicable AI risk management practices. For example, Section 5(b) of the Draft Memorandum already requires agencies to "review each use of AI that they are developing or using to determine whether it matches the definition of safety-impacting or rights-impacting." To make these impact determinations, an agency official will need to conduct some form of rudimentary AI impact assessment for all agency AI use cases. Rather than permit agencies to determine what procedures to follow when making these initial determinations, OMB could incorporate elements of its minimum practices at the determination stage to expand basic AI risk management to all AI use cases. For example, OMB could require an agency, when determining an AI system's designation as safety-impacting or rights-impacting, to report (1) its intended purpose and limitations, (2) the data used in the AI's design, development, training, testing, and operation, and (3) any human training or oversight measures undertaken.

OMB could seamlessly incorporate basic AI risk management practices into other reporting programs as well. Under Section 208 of the E-Government Act of 2002, for example, federal agencies are required to conduct, review, and publish PIAs before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form" or before initiating a new collection of information.[19] And while Section 208 dictates minimum requirements for PIAs, it grants OMB broad authority to determine the exact contents of PIAs.[20] Many government AI systems rely on the collection, transfer, and use of identifiable information to produce outputs like risk scores, predictions, recommendations, and inferences,[21] so when an agency uses AI to collect, process, store, or analyze identifiable

[18] Similar industry lobbying around AI designations has hindered European AI regulations. *See* Henshall, *supra* note 15; Perrigo, *supra* note 15.

[19] 44 U.S.C. 3501 note at 208(b)(1)(A); *see also* Memorandum from EPIC to the Exec. Off. of the President, the Vice President, and OMB on Integrating AI requirements into Section 208 Privacy Impact Assessments (Aug. 8, 2023), https://epic.org/wp-content/uploads/2023/10/EPIC-208-Memo.pdf [hereinafter "EPIC Section 208 AI Memo"].

[20] 44 U.S.C. 3501 note at 208(b)(3); *see also* EPIC Section 208 AI Memo.

[21] *See* Outsourced & Automated Report at 11–16; Screened & Scored Report at 11–15.

information, such use would cleanly fall within the definition of "information technology" covered by Section 208, requiring a PIA.[22] Integrating minimum AI impact requirements within OMB's existing PIA reporting program would not only align with OMB's statutory authority under the E-Government Act, but also align with the Biden-Harris Administration's priorities on responsible AI use.[23]

b. Recommendation Two: Prohibit Provably Harmful AI

OMB should include a list of AI use cases that are presumed noncompliant with the AI risk management practices set forth in the Draft Memorandum. For comprehensive AI oversight mechanisms to be effective, they must not only highlight the practices, policies, and procedures that agencies should follow, but also those that they should *avoid*. While the exact form of these prohibitions may vary, EPIC urges OMB to explicitly prohibit or deem presumptively noncompliant AI use cases that have proven to be particularly harmful and prone to algorithmic bias, including emotion recognition, biometric categorization, and one-to-many facial recognition.

Emotion recognition systems rely on the false premise that both universal emotions and a clear correlation between emotion and facial expression exist—a premise that has been repeatedly disproven.[24] Similarly, biometric categorization systems are based on the belief that certain physical characteristics can be linked to specific traits. This is essentially a form of digital phrenology.[25] Companies providing these AI systems have claimed to be able to predict anything from the likelihood of terrorist leanings to sexuality based solely on the analysis of facial features.[26]

[22] EPIC Section 208 AI Memo.
[23] *Id.*; *see also* Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence [hereinafter "Executive Order 14110"].
[24] Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, Atlantic (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-humanemotion/618696/; Lisa Feldman Barret et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 Ass'n for Psych. Sci., 1, 46 (2019), https://journals.sagepub.com/doi/pdf/10.1177/1529100619832930; *see also generally* Kuba Krys et al., *Be Careful Where You Smile: Culture Shapes Judgments of Intelligence and Honesty of Smiling Individuals*, 40 J. Nonverbal Behav. 101 (2016), https://link.springer.com/article/10.1007/s10919-015-0226-4; Charlotte Gifford, *The Problem with Emotion-Detection Technology*, New Econ. (June 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology.
[25] *See* Blaise Aguera y Arcas et al., *Physiognomy's New Clothes*, Medium (May 6, 2017), https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a.
[26] See Sally Adee, *Controversial Software Claims to Tell Your Personality From Your Face*, New Scientist (May 27, 2016), https://www.newscientist.com/article/2090656-controversial-software-claims-to-tellpersonalityfrom-your-face/; *Researchers are Using Machine Learning to Screen for Autism in Children*, Duke Pratt Sch. of Eng'g (July 11, 2019), https://pratt.duke.edu/about/news/amazon-autism-app-video; Paul

Lastly, one-to-many facial recognition systems—also known as biometric identification systems—involve indiscriminate and ongoing privacy violations of millions of people in the hopes of identifying a single suspect. As Senators Wyden, Markey, Padilla, and Booker put it, "[n]ot only does this violate individuals' privacy, but the inevitable false matches associated with one-to-many recognition can result in applicants being wrongly denied desperately-needed services for weeks or even months as they try to get their case reviewed."[27] Further, one-to-many recognition systems have been shown to falsely identify people of color as criminals at rates as much *as 100 times higher* than those for people of Eastern European descent.[28] All of these AI applications exhibit persistent and inherent inaccuracy, bias, and harm that are central and inseparable from the AI systems themselves; they cannot be corrected in a way that mitigates harm while permitting the AI application to continue.[29] These systems are harmful by their very nature and EPIC urges OMB to prohibit them expressly within its Draft Memorandum.

c. Recommendation Three: Incorporate Data Minimization Principles

OMB should incorporate explicit principles of data minimization into federal AI development, procurement, and use standards.[30] Given the data-dependent nature of AI development and use, as well as the number of potential risks and stakeholders impacted by AI systems, the risk of data misuse, cyber incidents, and other potential harm is high even when agencies evaluate the quality and appropriateness of data used. In other words, the *quantity* and *redundancy* of personal data used by many AI applications is also a source of serious AI risk.

Lewis, *"I was Shocked it was so Easy": Meet the Professor Who Says Facial Recognition Can Tell if You're Gay*, Guardian (July 7, 2018), https://www.theguardian.com/technology/2018/jul/07/artificialintelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis; Madhi Hashemi & Margaret Hall, *Criminal Tendency Detection from Facial Images and the Gender Bias Effect*, 7 J. Big Data, 1, 1 (2020), https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0282-4 (since retracted); Luana Pascu, *Biometric Software that Allegedly Predicts Criminals Based on Their Face Sparks Industry Controversy*, Biometric Update (May 6, 2020), https://www.biometricupdate.com/202005/biometric-software-that-allegedlypredicts-criminals-based-on-their-face-sparks-industry-controversy.

[27] Letter from Senators Wyden, Markey, Padilla, and Booker to FTC Chair Lina Khan 1 (May 18, 2022), https://epic.org/wp-content/uploads/2022/05/Letter-to-FTC-on-ID.me-deceptive-statements-051822.pdf.

[28] *Id.*

[29] *See* Section II, *infra.*

[30] *See* American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. § 101 (2022), https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf [hereinafter "ADPPA"]; Cons. Reps. & EPIC, How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking 3 (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

Most government AI use cases can be achieved without individuals' personal data being transferred to private vendors or used for an unrelated secondary purpose.[31] And in fact, an agency's collection, use, and transfer of personal data to private parties may already violate existing data privacy laws.[32] Incorporating data minimization into the Draft Memorandum is a viable, well-tested, and robust measure for preventing many forms of government AI risk.

Data collection, processing, and use are *prerequisites* for any government AI system, whether procured from the private-sector or developed by an agency. Much of the collection of personal data—both commercial and for government collection—happens so routinely and automatically that Americans have little to no knowledge of its scope[33]: everything from browsing the internet and using smart devices to filing your taxes and interacting with everyday government services can collect personal information that is then used to train and operate a wide variety of AI systems.[34] In fact, many of the most commonly procured government AI systems—systems used to, e.g., detect fraud, generate risk scores, and verify identities—are developed and sold by major data brokers that regularly and surreptitiously collect, process, repackage, and sell granular personal data.[35] Therefore, OMB cannot ensure responsible AI development, procurement, and use without also ensuring responsible government data collection, storage, transfer, and use

To capture and adequately mitigate the AI risks stemming from improper government data collection, processing, storage, transfer, and use, EPIC recommends amending the language to the data quality and appropriateness provision in Section 5(c)(iv)(A) of the Draft Memorandum as appears on the following page (**changes bolded in blue**):

[31] For example, an agency-developed AI system used only for its intended purpose would avoid unnecessary risk caused by relying on private AI vendors, transferring government data to private vendors, or passing sensitive personal data through an AI system trained on commercial data collected haphazardly. *See* EPIC, Comment on the FTC's Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 30–66 (Nov. 21, 2023), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf (discussing data minimization principles broadly) [hereinafter "EPIC FTC Commercial Surveillance Comment"].

[32] *See, e.g.*, E-Government Act of 2002, 44 U.S.C. § 3501 note; Privacy Act of 1974, 5 U.S.C. § 552a.

[33] EPIC FTC Commercial Surveillance Comment at 33–34.

[34] *Id.*; *see also* Kevin Collier, *U.S. Government Buys Data on Americans with Little Oversight, Report Finds*, NBC News (June 13, 2023), https://www.nbcnews.com/tech/security/us-government-buys-data-americans-little-oversight-report-finds-rcna89035; Justin Pot, *Tax Apps Collect Your Data: How Worried Should You Be?*, PC Mag. (Apr. 1, 2022), https://www.pcmag.com/news/tax-apps-collect-your-data; *cf. Privacy Impact Assessments*, EPIC, https://epic.org/issues/open-government/privacy-impact-assessments/ (last visited Dec. , 2023).

[35] *See* Outsourced & Automated Report at 14–16, 31–35, 38–40.

RECOMMENDATION

"3. *The quality****, appropriateness, and necessity*** *of relevant data*. Agencies must assess the quality of the data used in the AI's design, development, training, testing, and operation**; its fitness to the AI's intended purpose; and its necessity and proportionality to effect the AI's intended purpose.** If the agency cannot access such data after a reasonable effort to do so, it must obtain sufficient descriptive information from the AI or data provider to satisfy the reporting requirements in this paragraph. At a minimum, agencies must document:

a. the provenance and quality of the data for its intended purpose;
b. how the data is **necessary and proportional to the task being automated, the AI's intended purpose, and the AI's development, testing, and operation;**
c. whether the data contains sufficient breadth to address the range of real-world inputs the AI might encounter;
d. whether the data comes from an adequately reliable source; and
e. how errors from data entry, machine processing, or other sources are adequately measured and limited, to include errors from relying on AI-generated data as training data or model inputs.

Unless otherwise required by law, agencies must not collect, process, purchase, or transfer data for the purposes of developing, training, or using AI unless the collection, processing, purchasing, or transfer is limited to what is reasonably necessary and proportionate to effect a purpose permitted by law that benefits those to whom the data pertains."[36]

d. Recommendation Four: Adopt Additional Protections for Sensitive Personal Data

EPIC encourages OMB to include additional protections for sensitive personal data, including children's data; data pertaining to race, sex, ethnicity, religion, and national origin; and other similarly sensitive types of personal information. AI systems that use these categories of data are particularly vulnerable to inequitable or otherwise harmful outcomes—including data breaches and discrimination—and should always be considered rights-impacting.[37] For example, hiring

[36] *See* ADPPA; Cons. Reps. & EPIC, *supra* note 30.

[37] *See, e.g.*, Compl. for Permanent Inj. & Other Equitable Relief at 34–35*, FTC v. CompuCredit Corp.*, No. 1:08–CV–1976–BBM–RGV (N.D. Ga. Oct. 8, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/06/080610compucreditcmptsigned.pdf (FTC suit against credit card company that allegedly used undisclosed behavioral scoring algorithm to determine credit limitations based on consumer conduct); James Vincent, *The Invention of AI 'Gaydar' Could be the Start of Something Much Worse*, Verge (Sept. 21, 2017), https://www.theverge.com/2017/9/21/16332760/ai-sexualitygaydar-photo-physiognomy; Claudia Garcia-Rojas, *The Surveillance of Blackness: From the Trans-*

algorithms and automated workplace management systems can produce racially discriminatory employment determinations.[38] Criminal and pretrial risk scores can exacerbate racial disparities in sentencing and bail decisions.[39] And a wide variety of AI use cases—from fraud detection to facial recognition—can incorporate protected characteristics into automated decision-making in potentially harmful ways through "proxy variables" like ZIP codes and last names.[40]

Because of the heightened risk of harm that the collection, processing, and use of sensitive personal data implicates, EPIC advocates for a heightened *strict data minimization* standard for AI use cases involving sensitive personal data: agencies must only collect, process, transfer, or use personal data pertaining to a legally protected characteristic like race, sex, national origin, or age—as well as any personal data of individuals under 18—when *strictly necessary* to achieve a purpose permitted by law and intended to benefit those to whom the data pertains.[41]

Funding for AI Risk Management, Training, & Compliance

Responsive to Question 7

Responsible AI development, procurement, and use takes time and resources. Before agencies can ensure that AI use is safe, reliable, responsible, and trustworthy, they must, at minimum, (1) learn what data inputs an AI system requires, (2) learn how an AI system produces outputs, (3) train their employees on AI system uses and limitations, (4) test the AI system for accuracy, reliability, security, and lack of bias, (5) evaluate AI system performance across relevant, real-world environments, and (6) develop ongoing testing and oversight procedures to ensure that an AI system remains safe, responsible, and trustworthy over time.[42] For AI systems procured

Atlantic Slave Trade to Contemporary Surveillance Technologies, Truthout (Mar. 3, 2016), https://truthout.org/articles/thesurveillance-of-blackness-from-the-slave-trade-to-the-police/ (discussing Professor Simone Brown's research on how race and anti-Black colonial logics inform contemporary surveillance practices).

[38] EPIC FTC Commercial Surveillance Comment at 116–17; *see also* Miranda Bogen & Aaron Rieke, Upturn, Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias 21, 26, 28–29, 39 (2018), https://www.upturn.org/work/help-wanted/.

[39] *See* Ben Winters, EPIC, Liberty at Risk: Pre-trial Risk Assessment Tools in the U.S. 9–10 (2020), https://epic.org/documents/liberty-at-risk/; Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, ProPublica (2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[40] Outsourced & Automated Report at 17–20; *see also* Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa L. Rev. 1257 (2020), https://perma.cc/SC2T-8RHN; Ruha Benjamin, Race After Technology 1 (2019).

[41] *See* EPIC FTC Commercial Surveillance Comment at 176.

[42] *See* OSTP, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People 7, 18–20, 35, 46, 49–51 (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [hereinafter "Blueprint for an AI Bill of Rights"]; NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) 23, 26–27, 29–30, 32 (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [hereinafter "NIST AI RMF"].

from private developers, agencies must also ensure they have access to enough information to accomplish these tasks on an ongoing basis.[43] And these substantive oversight procedures must also pair with ongoing transparency and reporting mechanisms to ensure that OMB and the general public can hold agencies accountable for their AI use. All these tasks require resources, so funding for AI risk management must be at the core of any responsible AI use paradigm.

OMB has taken a strong stance on AI risk management funding by including explicit language within its Draft Memorandum requiring the "head of each covered agency… [to] consider the necessary financial, human, information, and infrastructural resources to carry out these responsibilities effectively, including providing or requesting resources via the budget process."[44] Despite this strong language, however, ensuring that agencies devote sufficient resources to AI risk management in practice may still pose a challenge. Following the passage of the E-Government Act of 2002, for example, federal agencies were required to conduct and report Privacy Impact Assessments (PIAs) when "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form" or "initiating a new collection of information" using information technology.[45] However, EPIC has uncovered several agencies that have failed to conduct and publish PIAs when required, including the Federal Bureau of Investigation, the Census Bureau, and the U.S. Postal Service.[46]

RECOMMENDATION

To ensure that agencies comply with the substantive requirements of the Draft Memorandum, OMB should consider **conditioning agency budget approvals and funding recommendations under the Draft Memorandum on ongoing compliance** with the Draft Memorandum's substantive provisions—and ongoing documentation proving that agencies are directing this dedicated funding directly and solely toward AI risk management.

[43] *See* Outsourced & Automated Report at 51–53.

[44] Draft Memorandum from Shalanda D. Young, OMB, to the President on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence 3 (Nov. 1, 2023), https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf [hereinafter "Draft OMB AI Guidance"].

[45] 44 U.S.C. § 3501 note at 208(b)(1)(A)(ii).

[46] *See, e.g.*, *EPIC v. USPS*, No. 1:21-cv-02156, 2022 WL 888183 (D.D.C. 2022); *EPIC v. Commerce*, 928 F.3d 95 (D.C. Cir. 2019); *EPIC v. FBI*, 72 F. Supp. 3d 388 (D.D.C. 2014).

AI Use Case Inventories

Responsive to Questions 6–8

EPIC applauds OMB's inclusion of long overdue, government-wide AI use case inventories within its Draft Memorandum. While several agencies have already begun to publish AI use case inventories[47] pursuant to Executive Order 13960,[48] the information included in existing AI use case inventories are thus far insufficient to ensure responsible AI development, procurement, and use. Some existing use case inventories, like that of the Department of Health and Human Services, only include a use case name, designated federal office, and 200-word summary of the AI system.[49] Others, like the Department of Energy's use case inventory, are riddled with blank entries.[50] Given the variety of AI use case inventories in both format and quality, OMB's AI use case inventory requirement has the potential to set a robust benchmark for responsible AI documentation across government.

AI use case inventories are valuable only insofar as they provide sufficient information to ensure agencies' compliance with their substantive AI risk management obligations. Inventory information should be granular enough for OMB, auditors, and concerned citizens to understand both how an agency is using its AI systems and how an agency is testing, evaluating, and mitigating AI risks. Anything less undermines government accountability, government transparency, and AI risk management.

[47] *See* Ben Winters, *Agencies Begin to Comply with 2020 Executive Order on AI Transparency*, EPIC Blog (Aug. 3, 2022), https://epic.org/agencies-begin-to-comply-with-2020-executive-order-on-ai-transparency/.

[48] Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, 85 Fed. Reg. 78939 (Dec. 3, 2020), https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

[49] *See* Dep't Health & Hum. Servs., Artificial Intelligence Use Cases – FY 2022 (2022), https://www.hhs.gov/sites/default/files/hhs-ai-use-cases-inventory.pdf.

[50] *See* Dep't Energy, Agency Inventory of AI Use Cases (2022), https://www.energy.gov/sites/default/files/2022-07/DOE_Agency_Inventory_of_AI_Use_Cases.pdf.

To ensure AI use case inventories complement other substantive AI risk management practices and incentivizes agency compliance with the Draft Memorandum, **OMB should require, at minimum, the following six (6) pieces of information within an AI use case inventory**:

1. **Agency determinations** that an AI system is safety-impacting or rights-impacting;

2. Agency **requests for extensions to or waivers** of OMB's minimum practices, alongside explanations or justifications;

3. **AI impact assessments**, alongside any documentation of the methods used and results produced.

4. Any agency **documentation of how an AI system was developed or procured**, including any contractors or vendors involved, any finalized contracts, any training methods used, and any pre-deployment testing, evaluation, validation, or verification completed;

5. The procedures for and results of any **ongoing AI testing** undertaken by the agency;

6. **Incident reports** following the identification of any errors, biases, or other documented harms of an agency AI system, alongside any remedial changes that the agency plans to adopt to mitigate the identified issue.[51]

RECOMMENDATION

[51] OMB may wish to consult existing incident reporting procedures from agencies like the National Transportation Safety Board (NTSB) for examples of what these reports could look like. *See* Nat'l Transp. Safety Bd., *Investigation Report*, NTSB.org, https://www.ntsb.gov/investigations/AccidentReports/Pages/Reports.aspx (last visited Dec. 5, 2023). At minimum, these reports should include (1) details about the documented risk or incident, (2) an analysis of any factual data, (3) evaluations of likely root causes, and (4) a remedial compliance plan to mitigate the identified issue.

In addition, EPIC recommends the following amendment to Section 3(a) of the Draft Memorandum, which draws on both existing federal AI guidelines[52] and EPIC's own research into effective AI oversight and accountability mechanisms[53] (**changes bolded in blue**):

RECOMMENDATION

"**AI Use Case Inventories**. Pursuant to Section 7225 of the Advancing American AI Act, and subject to the exclusions in that Act and Section 10.1(e) of the AI Executive Order, each agency (except for the Department of Defense and the Intelligence Community) must annually submit an inventory of its AI use cases to OMB and subsequently post a public version on the agency's website. OMB will issue detailed instructions for the inventory through its Integrated Data Collection process or an OMB-designated successor process. Beginning with the use case inventory for 2024, agencies will be required, as applicable, to identify and report additional detail on how they are using safety-impacting and rights-impacting AI, the risks—including risks to equity—that such use poses, how they are managing those risks, and any related extensions and waivers granted under. **These additional details must include, at minimum:**

a. The name of the AI system;
b. The intended uses and limitations of the AI system;
c. All required data inputs for the AI system;
d. A determination on whether the AI system is generative AI;
e. Documentation and results of all testing and evaluation procedures completed since the previous submission;
f. Any completed incident reports relevant to the AI system;
g. Documentation on AI system development or procurement, including information on related vendors, sources of data, and relevant contracts."

Under Section 5(c) of its Draft Memorandum, OMB also requires agencies to "provide public notice and plain-language documentation through the AI use case inventory," including documentation or links to the information "where people will interact with or be impacted by the AI."[54] **Whenever possible, EPIC urges OMB to ensure that as much information about**

[52] NIST, *NIST AI Risk Management Framework Playbook – Govern* 7 (Jan. 28, 2023), https://github.com/usnistgov/AIRMF/blob/nist-pages/govern/govern.pdf; Blueprint for an AI Bill of Rights at 21; *cf. also The Government is Using AI to Better Serve the Public*, AI.gov, https://ai.gov/ai-use-cases/ (last visited Dec. 5, 2023) (existing AI use case inventories).
[53] *See, e.g.*, Accountable Tech, AI Now Institute, EPIC, Zero Trust AI Governance (2023), https://ainowinstitute.org/wp-content/uploads/2023/08/Zero-Trust-AI-Governance.pdf; EPIC Generative AI Report.
[54] Draft OMB AI Guidance at 17–18.

agency AI risk management practices as possible is also made publicly available in a plain-language and approachable format—including all information suggested in the list above. Civil society organizations and concerned members of the public can and should play a role in holding agencies accountable for their compliance with the Draft Memorandum, but they cannot do anything unless they have access to information about what AI systems the federal government uses, how those systems impact them, and how federal agencies are managing the risks of AI use.

AI Impact Assessments

Responsive to Questions 6–8

Truly responsible AI requires rigorous, supported oversight infrastructure and careful moderation. Without oversight, measurable demonstrations of compliance efforts, and the possibility of enforcement or other legal liability, AI actors have few incentives to spend the time and resources necessary to conform their practices to the standards that OMB and individual agencies set out. Without actionable transparency and accountability mechanisms, there can be no public trust in the government's use of AI.

Building on existing federal AI guidelines[55] and EPIC's own research into effective AI oversight and accountability mechanisms,[56] EPIC recommends further amending Section 5(c)(iv) of the Draft Memorandum—as appears on the following page—to bolster OMB's oversight capabilities through more robust AI impact assessment requirements (**changes bolded in blue**, **previous data minimization amendment bolded in green**):

[55] NIST, *NIST AI Risk Management Framework Playbook – Govern* 7 (Jan. 28, 2023), https://github.com/usnistgov/AIRMF/blob/nist-pages/govern/govern.pdf; Blueprint for an AI Bill of Rights at 21; *cf. also The Government is Using AI to Better Serve the Public*, AI.gov, https://ai.gov/ai-use-cases/ (last visited Dec. 5, 2023) (existing AI use case inventories).

[56] *See, e.g.*, Accountable Tech, AI Now Institute, EPIC, Zero Trust AI Governance (2023), https://ainowinstitute.org/wp-content/uploads/2023/08/Zero-Trust-AI-Governance.pdf; EPIC Generative AI Report.

RECOMMENDATION

"3. *The quality****, appropriateness, and necessity*** *of relevant data*. Agencies must assess the quality of the data used in the AI's design, development, training, testing, and operation**; its fitness to the AI's intended purpose; and its necessity and proportionality to effect the AI's intended purpose.** If the agency cannot access such data after a reasonable effort to do so, it must obtain sufficient descriptive information from the AI or data provider to satisfy the reporting requirements in this paragraph. At a minimum, agencies must document:

a. the provenance and quality of the data for its intended purpose;
b. **the inputs and logics of the AI system;**
c. **the type or types of data generated by the AI system;**
d. how the data is **necessary and proportional to the task being automated, the AI's intended purpose, and the AI's development, testing, and operation;**
e. whether the data contains sufficient breadth to address the range of real-world inputs the AI might encounter;
f. whether the data comes from an adequately reliable source; and
g. how errors from data entry, machine processing, or other sources are adequately measured and limited, to include errors from relying on AI-generated data as training data or model inputs.
h. **The process and results of regular AI system validation studies;**
i. **Any downstream uses for AI system outputs beyond the system's intended purpose;**
j. **Any agency data management policies and procedures relevant to the AI system;**
k. **The process and results of any environmental impact statements or similar analyses regarding the AI system;**
l. **Any agency procedures for human review or interaction with the AI system;**
m. **The results of any risk-benefit analysis conducted for the AI system.**

Unless otherwise required by law, agencies must not collect, process, purchase, or transfer data for the purposes of developing, training, or using AI unless the collection, processing, purchasing, or transfer is limited to what is reasonably necessary and proportionate to effect a purpose permitted by law that benefits those to whom the data pertains."[57]

[57] *See* ADPPA; Cons. Reps. & EPIC, *supra* note 30.

EPIC has organized and published comparisons of impact assessments in current regulations, law, and proposed law.[58] While these impact assessment requirements vary, there are two notable consistencies throughout. **First**, in nearly all of the AI assessments introduced in state legislatures, assessments required (1) a description of the AI system's intended purpose and proposed use; (2) information on necessity of the automated decision-system; (3) a cost-benefit analysis weighing AI risks with benefits; (4) information regarding the effects of an AI system on civil, constitutional, and legal rights; (5) disparate impact evaluations; (6) risk mitigation plans; (7) data quality assessments; (8) performance or benchmark auditing requirements; and (9) bias audits or similar testing.[59] **Second**, to determine when AI assessments are required, laws or bills in Canada and the United Kingdom—as well as California, Vermont, and Washington—require AI assessments for *all* AI systems that contribute to or replace a decision-making process, rather than restricting AI assessments to categories like safety-impacting or rights-impacting AI.[60]

EPIC remains eager to assist OMB in finalizing protective and workable AI impact assessment and audit requirements to align government use of AI with the priorities of OMB and the Biden-Harris Administration.

Decommissioning Noncompliant AI

Responsive to Question 6

EPIC strongly supports OMB's inclusion of AI decommissioning requirements "[w]here the AI's risks to rights or safety exceed an acceptable level and where mitigation is not practicable."[61] Decommissioning or disgorging AI systems when mitigation fails has been a core element of several recent federal efforts to manage AI risks, including the White House Office of Science and Technology Policy (OSTP)'s Blueprint for an AI Bill of Rights,[62] the National Institute for Standards and Technology (NIST)'s AI Risk Management Framework,[63] and several recent Federal Trade Commission (FTC) enforcement actions.[64] Several AI and machine learning practitioners—including Amazon Web Services AI researchers Alessandro Achille, Michael Kearns, Carson Klingenberg, and Stefano Soatto—have also proposed model disgorgement and

[58] For a full table containing side-by-side comparisons of impact assessment requirements around the world, see Kara Williams, *Assessing the Assessments: Comparing Risk Assessment Requirements Around the World*, EPIC Blog (Dec. 4, 2023), https://epic.org/impact-comparison/.
[59] *Id.*
[60] *Id.*
[61] Draft OMB AI Guidance at 17.
[62] Blueprint for an AI Bill of Rights at 5, 15.
[63] NIST AI RMF at 23, 33.
[64] *See, e.g.*, Jevan Hutson & Ben Winters, *America's Next "Stop Model!": Model Disgorgement* 9–11, 14–16 (Priv. L. Scholars Conf. Draft Paper, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225003.

deletion as a best practice for responsible AI development and use.[65] Achille and colleagues argue that model disgorgement and deletion could "address a wide range of issues, such as reducing bias or toxicity, increasing fidelity, and ensuring responsible usage of intellectual property."[66]

Given the wide-ranging benefits of model decommissioning as a risk management practice, EPIC strongly encourages OMB to **expand the procedures, expectations, and oversight for AI decommissioning under its Draft Memorandum**, including, *inter alia*, provisions establishing a minimum acceptable level for all federal AI applications, independent review of agency AI use to identify systems in need of decommissioning, and an **interagency blacklist of decommissioned AI systems** to inform future agency decisions around AI development, procurement, and use.

RECOMMENDATION

AI Procurement Procedures and Contract Language

Responsive to Questions 1, 6, and 7

EPIC applauds OMB's inclusion of additional procurement requirements for federal AI procurement, particularly the requirements to keep procured AI transparent, maintain AI testing and risk management practices for procured AI, and promote competitive bidding. In fact, many of OMB's suggested procurement requirements mirror recommendations from EPIC's own research into government AI procurement.[67] EPIC's research highlighted to core barriers to responsible AI procurement: (1) procurement officials' lack of knowledge, access, and resources they need to properly oversee the AI procurement process and (2) noncompetitive procurement processes like cooperative purchasing that powerful AI vendors have used to capture government contracts without serious scrutiny.[68] OMB's draft AI procurement provisions are an important step toward overcoming both barriers. For example, OMB's provision encouraging agencies to "take appropriate steps to ensure that Federal AI procurement practices promote opportunities for competition among contractors and do not improperly entrench incumbents"[69] is in line with

[65] *See, e.g.*, Alessandro Achille et al., *AI Model Disgorgement: Methods and Choices*, arXiv (Apr. 7, 2023), https://arxiv.org/pdf/2304.03545.pdf.

[66] *Id.* at 1. For more on model disgorgement, decommissioning, and deletion, see Hutson & Winters, *supra* note 64.

[67] *See* Outsourced & Automated Report at 50–62.

[68] *See id.* at 32–36, 54.

[69] Draft OMB AI Guidance at 21.

EPIC's findings that cooperative purchasing agreements have been abused by powerful AI vendors like Deloitte and Thomson Reuters to entrench their position across agencies.[70]

Although OMB's Draft Memorandum goes further than other AI guidance to implement AI risk management into the procurement process, it currently ignores the power imbalance between several agency procurement offices and major AI vendors. For example, vendors may attempt to pressure procurement officials to ignore transparency or testing requirements within AI contracts or seek to market their products outside the scope of OMB's safety-impacting or rights-impacting designations. In practice, there is only so much an agency can do to monitor the AI systems they procure under existing contracts. From provisions that grant AI vendors exclusive rights to maintain and operate an AI system[71] to data privacy provisions that fail to restrict how vendors use AI outputs created using government data,[72] many AI contracts benefit vendors far more than agencies. These contracts reflect the relative power and knowledge of the contracting parties: because many agencies lack the expertise and resources to check or overwrite provisions that favor AI vendors, they often agree to contractual language that restricts or undermines their authority.

RECOMMENDATION

To support agency procurement offices in similar circumstances, EPIC encourages OMB to provide agencies with **sample contract language or similar templates** for responsibly navigating the AI procurement process and managing procured AI.[73] EPIC has identified three contractual provisions that OMB should focus on to maximize the ability of agency procurement officials to effectively manage the risks of procured AI:

1. Improving data oversight and control;
2. Imposing transparency and reporting requirements on vendors; and
3. Incorporating sunsetting clauses and procedures to transition ownership to agencies.

[70] *See* Outsourced & Automated Report at 33–35; *cf.* 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/.
[71] *See* Contract between D.C. Dep't Hum. Servs. and Pondera Solutions (2020), https://epic.org/wp-content/uploads/2022/06/EPIC-21-06-25-DC-DHS-FOIA-20210719-Production-Pondera-Contract.pdf.
[72] *See* Carahsoft Master Agreement with Aisera Pricing Schedule (2016), https://epic.org/wp-content/uploads/2023/09/Carahsoft-NASPO-Master-Agreement-Aisera-Pricing-Schedule.pdf.
[73] EPIC attorneys are involved with the IEEE's draft AI procurement standard, P3119. *See Standard for the Procurement of Artificial Intelligence and Automated Decision Systems*, IEEE SA, https://standards.ieee.org/ieee/3119/10729/ (last visited Dec. 5, 2023). EPIC would be happy to discuss responsible AI procurement further.

a. *Provision One: Improving Data Oversight and Control*

EPIC's research into AI procurement suggests that government AI contracts often fail to consider what secondary uses a vendor may have for agency data, meaning that vendors could use the data agencies provide (or inferences derived from that data) for other purposes after the contract requirements are met.[74] Stronger data oversight provisions in government AI contracts can ensure that AI vendors do not misuse or profit off government data in secondary commercial markets. However, the opposite is also true: agencies should not attempt to use AI contracts to access vendor data beyond what government agencies are entitled to collect directly.

Of the 621 AI contracts EPIC reviewed, few included strong data protection and control provisions.[75] However, EPIC has identified at least one example of strong contract language concerning government data oversight and control—language taken from a contract between the Illinois Department of Employment Security and Pondera Solutions, a Thomson Reuters subsidiary:

> *All work performed or supplies created by Vendor under this contract, whether written documents or data, goods or deliverables of any kind, shall be deemed work for hire under copyright law and all intellectual property and other laws, and the [Contracting Agency] is granted sole and exclusive ownership to all such work, unless otherwise agreed in writing.*[76]

While EPIC does not believe this language should be adopted as-is, the Illinois AI contract goes further than many to ensure that data inferences, AI models, and other resources generated by a vendor under the contract remain solely within the government's control.

b. *Provision Two: Imposing Transparency and Reporting Requirements*

While researching AI procurement, EPIC identified several instances in which agencies outsourced the entire operation of AI systems to vendors. These contracts—often described as "software as a service" contracts—make it difficult for agency officials to understand how procured AI systems work or why they produce certain outputs.[77] Without direct access to and

[74] *See* Carahsoft Master Agreement with Aisera Pricing Schedule (2016), https://epic.org/wp-content/uploads/2023/09/Carahsoft-NASPO-Master-Agreement-Aisera-Pricing-Schedule.pdf.
[75] *See* Outsourced & Automated Report at 41–48; *Outsourced & Automated*, EPIC, https://epic.org/outsourced-automated/ (full contract database available for reference).
[76] *Id.* at 43–44; *see also* Contract between Ill. Dep't Emp. Sec. and Pondera Solutions (2020), https://epic.org/wp-content/uploads/2022/06/EPIC-21-10-22-IL-IDES-FOIA-20211110-Illinois-Pondera-Contract.pdf.
[77] *See* Contract between D.C. Dep't Hum. Servs. and Pondera Solutions (2020), https://epic.org/wp-content/uploads/2022/06/EPIC-21-06-25-DC-DHS-FOIA-20210719-Production-Pondera-Contract.pdf.

independent oversight of the processes used to produce AI outputs, agencies cannot ensure that the AI systems they procure and use are fair, accurate, or reliable.

Robust and independent audits of AI systems and their outputs are the gold standard for responsible, transparent AI use[78]—and ongoing audit requirements like those found in Section 5(c)(iv)(C) of the Draft Memorandum can and should be incorporated into government AI contracts. These audit requirements could come into play at two stages of the AI procurement process. **First**, AI vendors and contractors could be required to disclose a detailed description of their AI system's capabilities, data requirements, intended uses, and limitations when they bid on a federal contract.[79] Agency procurement officials could then compare AI systems' capabilities with their agencies' needs to determine whether the AI system is appropriate—or even whether an AI system is necessary. **Second**, state agencies could include contractual provisions requiring AI audits as part of the bidding process or during the contract term.[80]

Only a few of the 621 AI contracts EPIC reviewed contained an AI audit requirement. However, EPIC has identified at least one example of strong contract language concerning independent AI audits—language taken from a contract between the Michigan Department of Technology, Management, and Budget and Deloitte Consulting:

> *Contractor will deposit with [an] escrow agent… the Source Code for the [AI System Software], as well as the Documentation and names and contact information for each author or other creator of the [AI System Software] … At [Agency's] request and expense, the escrow agent may at any time verify the [Source Code,] compar[e] it to the [AI System Software], and review[] the completeness and accuracy of any and all material.*[81]

While EPIC does not believe this language should be adopted as-is, the Michigan AI contract goes further than many to ensure that vendor-provided AI systems are independently audited throughout the contract term.

[78] For example, the White House recommends audits as part of the Blueprint for an AI Bill of Rights, and NIST includes audits, testing, and evaluation as core features of its AI Risk Management Framework. Blueprint for an AI Bill of Rights at 20–21, 24, 38; NIST AI RMF at 16, 19, 26–30.
[79] *See* Outsourced & Automated Report at 52–53.
[80] *Id.*
[81] *Id.* at 48; *see also* Contract between Mich. Dep't Tech., Mgmt., & Budget and Deloitte Consulting (2023), https://epic.org/wp-content/uploads/2023/09/Michigan-Deloitte-uFACTS-Contract.pdf.

c. *Provision Three: Incorporating Sunsetting Clause and Procedures to Transition Ownership to Agencies*

EPIC identified several government AI contracts that gave vendors complete and exclusive control over the operation of the AI system. These contracts, which can last for several years, restrict agencies' ability to change how they use AI systems and which vendors they use—unless they spend a large amount of money to terminate contracts and initiate another procurement process.[82] Although EPIC was unable to find contract language supporting AI system sunsetting and ownership transition, these provisions can ensure that agency officials maintain sufficient control over government AI systems to comply with the requirements of OMB's Draft Memorandum.

II. Agencies Should Not Adopt AI Solely for AI's Sake

We recognize the desire of the White House to promote the research and development of AI used for beneficial purposes. However, EPIC urges OMB to remove provisions that explicitly call for the adoption of AI in general, rather than considering the best approach for each issue. As several federal government agencies—as well as President Biden and Vice President Harris—have recognized in no uncertain terms, there are serious and ever-present issues of discrimination and inaccuracy with AI use today.[83] The administration should not make an unforced error by justifying the rapid research and development of AI "solutions" in search of problems. If innovation must be the primary goal, rather than civil rights and privacy protection, there must be a more balanced perspective of what true innovation is—one that focuses on responsibility and integrates innovative methods for AI risk management throughout the AI lifecycle.

[82] For example, the Michigan Unemployment Insurance Agency was forced to abandon its $47 million MiDAS system after litigation revealed thousands of false fraud allegations. *See Michigan Unemployment Insurance False Fraud Determinations*, Benefits Tech Advoc. Hub, https://www.btah.org/case-study/michigan-unemployment-insurance-false-fraud-determinations.html. To replace the faulty system, Michigan paid Deloitte $59 million. *See* Contract between Mich. Dep't Tech., Mgmt., & Budget and Deloitte Consulting (2023), https://epic.org/wp-content/uploads/2023/09/Michigan-Deloitte-uFACTS-Contract.pdf.

[83] Vice President Harris, Remarks by Vice President Harris on the Future of Artificial Intelligence at the U.S. Embassy in London (Nov. 1, 2023), https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/11/01/remarks-by-vice-president-harris-on-the-future-of-artificial-intelligence-london-united-kingdom/; Khari Johnson, *Joe Biden Wants US Government Algorithms Tested for Potential Harm Against Citizens*, Wired (Nov. 1, 2023), https://www.wired.com/story/joe-biden-wants-us-government-algorithms-tested-for-potential-harm-against-citizens/; Rohit Chopra et al., Joint Statement on Enforcement Against Discrimination and Bias in Automated Systems (Apr. 25, 2023), https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

The need to protect innovation is often raised as a reason to oppose or weaken proposed privacy protections.[84] However, OMB must recognize that innovation in AI guardrails, oversight mechanisms, evaluation methods, and risk management practices must come before innovation in AI models. Expediting AI research and development is not responsible AI innovation, but *irresponsible* AI innovation. For federal AI development, procurement, and use to be truly responsible, the United States must instead focus on being first-in-class for AI oversight, risk management, and harm prevention.

AI Systems are Frequently Discriminatory

Responsive to Questions 3–4

Numerous governmental bodies, including NIST, the Government Accountability Office (GAO), OSTP, and many others, have published reports outlining key issues with AI, such as bias, discrimination, and inaccuracy.[85] As publicly funded institutions, these bodies and other agencies are well positioned to be a trusted source for expertise on matters of AI accuracy, bias, and disparate impact. EPIC urges OMB to leverage the expertise and public trust of federal agencies to publish key information about how AI is used in different sectors, and how that use affects the public.

For example, in 2022, NIST published Special Publication 1270, "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence," which identifies three types of bias that infiltrate AI—systemic bias, human bias, and statistical or computational bias—and provides recommendations to mitigate these biases for AI developers and users.[86]

Another NIST study, published in 2020, reviewed 189 algorithms from 99 developers and found that facial recognition technology had widespread issues identifying non-White faces.[87] Patrick Grother, a NIST computer scientist who worked on the report, said, "While it is usually

[84] *See*, *e.g.*, Calli Schroeder et al., *We Can Work It Out: The False Conflict Between Data Protection and Innovation,* 20 Colo. Tech. L. J. 251, 256–60 (2023), https://ctlj.colorado.edu/wp-content/uploads/2023/02/3-We-Can-Work-it-Out_091922.pdf.

[85] *See generally* GAO, GAO-21-519SP, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities (2021), https://www.gao.gov/assets/gao-21-519sp.pdf; GAO, GAO-21-7SP, Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care (2020), https://www.gao.gov/products/gao-21-7sp; Blueprint for an AI Bill of Rights at 23–29; Reva Schwartz et al., NIST, Towards a Standard for Identifying and Managing Bias in Artificial Intelligence (NIST Special Publ'n 1270, Mar. 15, 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

[86] Schwartz et al., *supra* note 85.

[87] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NIST (May 18, 2020), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

incorrect to make statements across algorithms, we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied."[88]

AI Systems are Frequently Inaccurate

Responsive to Questions 3–4

Automated systems, encompassing both generative and non-generative modalities, confront substantial accuracy challenges that necessitate vigilant human intervention.[89] Despite advancements in AI language generation, image recognition, and decision making, AI systems are intrinsically susceptible to fallibility, particularly when confronted with intricate or nuanced scenarios.[90] Generative AI models like GPT-4 and DALL-E 2 exhibit a capacity for contextually coherent yet fundamentally inaccurate information generation. The absence of genuine comprehension within these models renders them susceptible to producing misleading or erroneous content, particularly in response to ambiguous inquiries or situations characterized by incomplete data. Due to the importance of many interactions with government, these results are particularly dangerous.

Automated decision-making within governmental services is susceptible to AI bias and often proves incapable of accurately navigating diverse and dynamic nature of real-world application contexts.[91] These systems heavily rely on training data, and if the data incorporated during their development is biased or incomplete, consequential inaccuracies may emerge in AI predictions and decisions.[92] The innate inflexibility of AI systems to adapt to unforeseen circumstances renders them unreliable in contexts where adaptability is paramount. The

[88] *Id.*

[89] Arun Shastri, *Generative AI Errs Differently Than Classical AI,* Forbes (Sept. 4, 2023), https://www.forbes.com/sites/arunshastri/2023/09/04/generative-ai-errs-differently-than-classical-ai/.

[90] Oceane Duboust, *Unreliable Research Assistant? False Outputs from AI Chatbots Pose Risk to Science, Report Says,* Euronews (Nov. 20, 2023), https://www.euronews.com/next/2023/11/20/unreliable-research-assistant-false-outputs-from-ai-chatbots-pose-risk-to-science-report-s; Tate Ryan-Mosley, *Catching Bad Content in the Age of AI*, MIT Tech. Rev. (May 15, 2023), https://www.technologyreview.com/2023/05/15/1073019/catching-bad-content-in-the-age-of-ai/ (explaining how generative AI's difficulty handling nuanced information presents problems for content moderation).

[91] *See* Matt Burgess et al., *This Algorithm Could Ruin Your Life*, Wired (June 3, 2023), https://www.wired.co.uk/article/welfare-algorithms-discrimination; Stephanie Wykstra, *Government's Use of Algorithm Serves Up False Fraud Charges*, Undark (June 1, 2020), https://undark.org/2020/06/01/michigan-unemployment-fraud-algorithm/; Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

[92] *See* Mona Rakibe, *The Significance of Data Quality in the World of Generative AI*, Medium (June 21, 2023), https://mona-rakibe.medium.com/the-significance-of-data-quality-in-the-world-of-generative-ai-5f84eb524299.

unwillingness of AI developers to devise their systems in a way that explains the reasoning for the output of a system leads to an impossibility of accountability.[93]

AI Systems Perpetuate Harmful Data Practices

Responsive to Questions 2–4

AI systems are tools with specific uses and limitations, not general-purpose tools that agencies can apply to every problem. Defining problems that need AI is crucial for any AI innovation or adoption to be responsible.

Agency adoption of Generative AI poses privacy risks.[94] These risks are inherently harmful, but also lead to compounding harms. Many generative AI tools use models built on data scraped from publicly available websites.[95] This information often includes personal information posted on social media and other websites.[96] When companies scrape personal information and use it to create generative AI tools, they undermine consumers' control of their personal information by using the information for a purpose for which the consumer did not consent. The individual may not have even imagined their data could be used in the way the company intends when the person posted it online.[97] Individual storing or hosting of scraped personal data may not always be harmful in a vacuum, but there are many risks. Multiple datasets can be combined in ways that cause harm: information that is not sensitive when spread across different databases can be extremely revealing when collected in a single place, and it can be used to make inferences about a person or population.[98] Even "anonymized data" has been shown to be easily tied to a

[93] *See* Blueprint for an AI Bill of Rights at 21, 45.

[94] Security Staff, *Data Privacy Among Top Concerns for Workplace Generative AI Use*, Sec. Mag. (Oct. 16, 2023), https://www.securitymagazine.com/articles/100028-data-privacy-among-top-concerns-for-workplace-generative-ai-use; Simon Fondrie-Teitler & Amritha Jayanti, *Consumers Are Voicing Concerns About AI*, FTC Tech. Blog (Oct. 3, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/10/consumers-are-voicing-concerns-about-ai; Lily Li, *International: Privacy Implications for Organizations Using Generative AI*, OneTrust DataGuidance (June 2023), https://www.dataguidance.com/opinion/international-privacy-implications-organizations; D. Reed Freedman Jr. et al., *Data Scraping, Privacy Law, and the Latest Challenge to the Generative AI Business Model*, ArentFox Schiff (July 17, 2023), https://www.afslaw.com/perspectives/privacy-counsel/data-scraping-privacy-law-and-the-latest-challenge-the-generative-ai.

[95] Sara Morrison, *The Tricky Truth About How Generative AI Uses Your Data*, Vox (July 27, 2023), https://www.vox.com/technology/2023/7/27/23808499/ai-openai-google-meta-data-privacy-nope; *see also* Thomas Claburn, *How to Spot OpenAI's Crawler Bot and Stop it Slurping Sites for Training Data*, Register (Aug. 8, 2023), https://www.theregister.com/2023/08/08/openai_scraping_software/.

[96] Geoffrey Fowler, *Your Instagrams are Training AI. There's Little You Can Do About It*, Wash. Post (Sept. 27, 2023), https://www.washingtonpost.com/technology/2023/09/08/gmail-instagram-facebook-trains-ai/.

[97] *Id*.

[98] *See* Boris Lubarsky, *Re-Identification of "Anonymized Data"*, 1 Geo. L. Tech. Rev. 202, 211 (2017), https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/; Sandra Wachter

specific individual.[99] And because scraping makes a copy of someone's data as it existed at a specific time, the company also takes away the individual's ability to alter or remove the information from the public sphere.

The privacy harms that follow from indiscriminate scraping of personal information for AI training data also create potential chilling effects for confused or concerned consumer.[100] Basic data minimization principles dictate that peoples' personal information should only be collected or used for the specific purpose for which each person provided the information.[101] But there are currently no statutes that prohibit companies from scraping people's personal information and using it to train generative AI tools.

Privacy laws in the U.S. exempt most publicly available information from regulation based on a concern that the collection and use of this information is protected by the First Amendment.[102] However, data brokers and AI companies scrape more than just publicly available information when building AI tools, regularly violating individual users' privacy.[103] In drafting regulations about potential agency use of these tools, OMB must be careful not to encourage extractive, invasive, or otherwise harmful data practices by agencies or AI developers seeking to enrich their underlying AI models with individuals' or government data.

OMB Should Revise Provisions Promoting AI Adoption for AI's Sake

Responsive to Questions 2–4

Much of Section 4 of the Draft Memorandum encourages AI adoption for AI adoption's sake, but OMB should revise its Draft Memorandum to instead reflect the concerns around responsible AI use and risk management described above. It is inappropriate for OMB to encourage the use of a specific modality, especially one as risky as AI, without sufficient regard

& Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, Colum. Bus. L. Rev., no. 2, 2019, at 502–520, https://journals.library.columbia.edu/index.php/CBLR/article/view/3424/1370.

[99] Lubarsky, *supra* note 98, at 208–12.

[100] Moritz Buchi et al., *The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda*, Big Data & Soc'y (Jan. 6, 2022), https://journals.sagepub.com/doi/10.1177/20539517211065368.

[101] Cons. Reps. & EPIC, *supra* note 30.

[102] David Stasis & Stacey Weber, *How Do the CPRA, CPA, VCDPA Treat Publicly Available Information?*, Husch Blackwell (Jan. 27, 2022), https://www.bytebacklaw.com/2022/01/how-do-the-cpra-cpa-vcdpa-treat-publicly-available-information/.

[103] *See, e.g.*, Müge Fazlioglu, *Training AI on Personal Data Scraped from the Web*, IAPP (Nov. 8, 2023), https://iapp.org/news/a/training-ai-on-personal-data-scraped-from-the-web/; EPIC, Comment on the CFPB's Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information (July 14, 2023), https://epic.org/wp-content/uploads/2023/07/EPIC-CFPB-data-brokers-RFI-comments-071423.pdf.

or safeguards for meaningful oversight. EPIC has four suggested changes to the Draft Memorandum.

First, from Section 3(b) of the Draft Memorandum, the below tasks are assigned to Chief AI Advisors. On the following page, EPIC recommends maintaining the relationship between AI adoption and specific circumstances of use and need (**changes bolded in blue, deletions crossed out**):

H. identifying and **instituting the requisite oversight necessary to achieve truly** responsible use of AI in the agency, including through ~~**the advancement of AI-enabling enterprise infrastructure,**~~ workforce development measures, policy, and other resources for AI innovation;

I. advocating within their agency and to the public **in plain language** on **proposed AI use cases that align with the agency's mission and assist operations;**

RECOMMENDATION

Second, EPIC is concerned that the introductory paragraph of Section 4 of the Draft Memorandum encourages agencies to 'move fast and break things,' when in fact this is in tension with responsible AI use by a government that works for the people and has immense obligation. Here, EPIC's recommendations hinge on ensuring the oversight and evaluation structure is supported—and that those developing and deploying AI are integrated into the relevant teams and processes where those AI systems will be instituted (**changes bolded in blue**):

"Agencies should create internal environments where those developing and deploying AI have flexibility **and opportunities to build subject matter expertise relevant to managing AI risk. These internal environments should be integrated into the appropriate agency teams to achieve** AI innovation **that is appropriate to the needs of the agency** and **prioritizes** risk management **throughout the AI lifecycle**."

RECOMMENDATION

Third, in Section 4(a) of the Draft Memorandum, OMB currently requires CFO Act agencies to "remove barriers to the use of AI." In Section 4(b), this phrase is used again, but with the word responsible included. **EPIC recommends that OMB delete both instances of the phrase or reorient the phrase's language around *support* for proper safeguards and oversight mechanisms as foundations for responsible AI innovation.**

Fourth, EPIC is deeply concerned at the promotion of generative AI as a technology worth adopting in and of itself. In Section 4(b)(v) of the Draft Memorandum, OMB encourages agencies to "assess potential beneficial use cases of generative AI in their missions and establish adequate safeguards and oversight mechanisms that allow generative AI to be used in the agency without posing undue risk."[104] **EPIC urges OMB to delete this provision entirely or reword it substantially to account for the severe privacy, accuracy, and bias concerns that generative AI technologies have demonstrated.**[105] This provision, as well as most of the Section 4 does work for AI companies by legitimizing the use and development of AI.

III. OMB Must Prioritize Transparency & Accountability

Responsive to Questions 2 and 8

RECOMMENDATION

OMB guidance without compliance is ineffective, and agency compliance without transparency risks being unaccountable. To ensure that OMB's Draft Memorandum effectively advances responsible government AI development and use, EPIC urges OMB to:

1. carefully consider how it could **use its existing budgetary and oversight authorities to incentivize or mandate strict compliance** amid differing agency priorities and interpretations of OMB's guidance;
2. revisit compliance protocols for and coordination with related, existing reporting requirements like **privacy impact assessments (PIAs) under the E-Government Act of 2002**;[106] and
3. **expand the scope and accessibility of information** that agencies are expected to make publicly available.

As discussed in Section II, *supra*, the mere existence of minimum AI risk management practices and OMB reporting requirements[107] will not ensure agency compliance. Despite decades-

[104] *Cf.* Executive Order 14110.
[105] *See generally* EPIC Generative AI Report.
[106] 44 U.S.C. § 3501 note.
[107] The Draft Memorandum currently requires covered agencies to provide OMB with, e.g., (1) the identities of their appointed Chief AI Officers (CAIOs), (2) their compliance plan under the Draft Memorandum or a "written determination that the agency does not use and does not anticipate using covered AI," (3) an inventory of their AI use cases, (4) any agency-specific lists concerning safety-impacting or rights-impacting AI use

old PIA requirements under the E-Government Act of 2002,[108] for example, many federal agencies still fail to generate and publish PIAs when required.[109] To incentivize compliance with the Draft Memorandum and Executive Order 14110, EPIC urges OMB to condition agency budget approvals and funding recommendations on compliance with all minimum practices and reporting requirements under the Draft Memorandum, including conditions on including agency budget requests within consolidated budget proposals prepared for the President pursuant to the Budget and Accounting Act of 1921.[110] Additionally, EPIC encourages OMB to prioritize review of agency determinations that AI systems are *not* safety-impacting or rights-impacting, as well as waivers of minimum practices and other related decisions concerning the applicability of the Draft Memorandum to an agency's practices. Historically, agencies have faced less OMB scrutiny for deregulatory measures than pro-regulatory measures,[111] but given the time and resources required to adequately comply with the Draft Memorandum, many agencies will be heavily incentivized to underreport AI use cases and deprioritize ongoing AI testing and evaluation measures even in circumstances where serious AI risks remain. Strong OMB oversight—built atop stringent reporting requirements and independent review—will be crucial for ensuring responsible AI development, procurement, and use throughout government.

The Draft Memorandum's minimum practices and reporting requirements do not exist in a vacuum either. Agencies are already obligated to document and report to OMB a large array of information related to their data and technology needs under statutes like the E-Government Act of 2002.[112] To ensure these other oversight and reporting requirements complement, rather than compete with, agency compliance with the Draft Memorandum, EPIC encourages OMB to revisit existing compliance and reporting programs to determine how agency CAIOs and similar officials should coordinate overlapping compliance requirements and effectively manage limited resources. For example, EPIC recently published a memorandum detailing how AI impact assessment requirements could be incorporated into PIAs under the E-Government Act.[113] OMB could

cases, (5) any agency determinations—or reversals of determinations—that an AI use case is not safety-impacting or rights-impacting and thus need not be subject to the minimum practices listed within the Draft Memorandum, (6) any documentation of agency implementation of the minimum practices listed within the Draft Memorandum, and (7) any waivers from minimum practices granted by the agency's CAIOs, which must detail the scope, justifications, and supporting evidence. Draft OMB AI Guidance at 4, 10–11, 13–15, 26.

[108] *Id.*

[109] *See, e.g.*, *EPIC v. USPS*, No. 1:21-cv-02156, 2022 WL 888183 (D.D.C. 2022); *EPIC v. Commerce*, 928 F.3d 95 (D.C. Cir. 2019); *EPIC v. FBI*, 72 F. Supp. 3d 388 (D.D.C. 2014). For more on EPIC's work involving PIAs, see *Privacy Impact Assessments*, EPIC, https://epic.org/issues/open-government/privacy-impact-assessments/ (last visited Dec. 5, 2023).

[110] *See* 31 U.S.C. §§ 1104, 1105, 1108.

[111] *See* Nicholas Bagley & Richard L. Revesz, *Centralized Oversight of the Regulatory State*, 106 Colum. L. Rev. 1260, 1271 (2006), https://www.jstor.org/stable/4099416.

[112] 44 U.S.C. § 3501 note.

[113] EPIC Section 208 AI Memo.

similarly publish guidance clarifying whether and how PIA requirements and related OMB guidance relates to the minimum practices and reporting requirements under the Draft Memorandum. If more expansive implementations of OMB's oversight and budgetary authorities can pressure agencies to comply with the minimum practices and reporting requirements of the Draft Memorandum, coordinating compliance with other agency programs and reporting regimes will help lower barriers to adequate and ongoing compliance.

Lastly, EPIC urges OMB to incorporate the public as a co-evaluator and source of pressure for agencies through increased transparency efforts around agency compliance with the Draft Memorandum. Civil society organizations like EPIC, as well as concerned citizens and independent researchers, can serve a valuable role as auditors, evaluators, co-regulators, researchers, and sources of pressure for agencies conducting the minimum practices and reporting requirements outlined in OMB's Draft Memorandum—but only if we have access to key information about federal AI development, procurement, and use. To the extent possible under existing laws, EPIC urges OMB to make public all procedures, documentation, compliance plans, testing results, and AI impact assessments produced by agencies under the Draft Memorandum so organizations like EPIC and academic researchers can evaluate agency practices, flag issues, and suggest innovative paths forward for federal AI risk management.

IV. OMB Should Narrowly Construe National Security Exemptions

Responsive to Questions 3 and 5

EPIC urges OMB to make every effort to narrowly define national security and other exempted uses to increase transparency and accountability around the most dangerous AI systems. Many of the most dangerous systems—those that violate the principles espoused in Executive Order 14410—are the very ones that need a meaningful public assessment. These systems are also likely to be used in part for ostensible national security purposes.[114] Without

[114] GAO, GAO-21-386, DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System 7 (2021), https://www.gao.gov/assets/gao-21-386.pdf (reporting that DHS's HART/IDENT biometric database is used for verifying identity of persons in national security matters); Sam Biddle, *How Peter Thiel's Palantir Helped the NSA Spy on the Whole World*, Intercept (Feb. 22, 2017), https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/; EPIC et al., Comments on Use of HHS Information Collection for Immigration Enforcement (Nov. 6, 2018), https://www.scribd.com/document/392614190/November-6-2018-Comments-to-HHS-and-DHS (explaining how information collected by HHS could be used to harm immigrant communities and in particular vulnerable children).

strong guardrails on national security exemptions, agencies may use these exemptions to avoid oversight altogether.

OMB should interpret the exceptions outlined in the Advancing American AI Act[115] narrowly by:

1. adopting a **use-case approach** to defining national security systems;
2. explicitly **requiring review of dual-use systems**; and
3. requiring agencies to **justify the rationale behind exempting systems** for national security reasons.

RECOMMENDATION

The Draft Guidance outlines several carveouts from the requirements of the guidance for national security purposes. The "Intelligence Community" is fully exempted from the Guidance under the Advancing American AI Act, while the Department of Defense (DoD) is partially exempted. Agencies outside the intelligence community can still claim an exemption which extends to AI "when it is used as a component of a national security system".[116] The Intelligence Community, as statutorily defined, covers both freestanding agencies like the National Security Agency (NSA), and agency subcomponents like the Office of Information and Analysis (I&A) withing the Department of Homeland Security (DHS), the Bureau of Intelligence and Research in the State Department, and "intelligence elements" of the armed forces, the DEA, and the FBI.[117] For agencies that are fully exempted like the NSA, OMB must still be careful not to exempt systems shared between agencies from all scrutiny. The task is more difficult when considering exempted sub-components in otherwise covered agencies, like DHS' I&A. Here OMB should be especially careful to ensure that agencies do not use these exemptions to avoid scrutiny by misclassifying their AI systems because of de minimis national security or intelligence community involvement.

Without careful guardrails and oversight from OMB, there is a substantial risk that agencies will designate all systems with some minimal national security purpose as exempted from the Draft Guidance, a loophole that could swallow the rule. By statute, "national security systems" are defined broadly to include "any information system" used by an agency where the "the function, operation or use of" the system "involves intelligence activities."[118] The State Department's Visa

[115] 40 U.S.C. § 11301 note; Pub. L. No. 117-263, 136 Stat. 3668.
[116] Draft OMB AI Guidance at 3 (Section 2(c)).
[117] 50 U.S.C. § 3003.
[118] 44 U.S.C. § 3552(b)(6)(A).

Records System (SORN State-39)[119] and Consular Consolidated Database[120] illustrate the risk that overbroad exemptions will fail to protect a substantial number of individuals from rights-impacting and harmful AI systems.

Visa Records is the overarching system used by the State Department to hold information on everyone who applies for a visa to visit the U.S., individuals who sponsor visa-holders, and a broad array of relevant information collected from various sources. The system holds sensitive personal information, biometrics like fingerprints and facial images, and extensive records. Visa Records lists routines users including several agencies within the Intelligence Community, and is marked as both a Classified and Unclassified system.[121] The Consular Consolidated Database is the State Department's overarching records system for both U.S. persons and non-U.S. persons, housing sensitive personal information including biometric data.[122] The CCD system also "serves as a gateway" to the State Department's facial recognition system.[123] CCD is integrated with other databases across the federal government, including DHS's massive biometrics data HART/IDENT and is accessible via information sharing memoranda of understanding with intelligence community agencies.[124]

Together these systems hold records on hundreds of millions of people and are used for substantial rights-impacting purposes like determining visa eligibility and screening for access to consular services for American citizens.[125] AI used for facial recognition and data analytics run off these systems collectively impacts millions of Americans and people around the world every year.[126] These systems are used mainly for straightforward determinations on access to services

[119] System of Records Notice Visa Records, State-039, 83 Fed. Reg. 280362 (Nov. 8, 2021), https://www.state.gov/wp-content/uploads/2021/11/State-39-Visa-Records-SORN-Web-Post-2021.pdf [hereinafter "Visa Records SORN"].

[120] U.S. Dep't of State, Privacy Impact Assessment for Consular Consolidated Database (CCD) (2022), https://www.state.gov/wp-content/uploads/2023/05/Consular-Consolidated-Database-CCD-PIA.pdf [hereinafter "CCD PIA"].

[121] Visa Records SORN at 1, 3.

[122] CCD PIA at 2.

[123] U.S. Dep't of State, Privacy Impact Assessment for Consular Consolidated Database (CCD) at 2 (2015), https://2009-2017.state.gov/documents/organization/242316.pdf; 2022 CCD PIA at .

[124] *See EPIC v. State Department (Facial Recognition Database)*, No. 19-1468 (D.D.C. Mar. 12, 2019), https://epic.org/documents/epic-v-state-department-facial-recognition-database/. EPIC successfully obtained many of the memoranda of understanding allowing other agencies access to CCD through a FOIA case, revealing for the first time the full extent to which CCD is used by the federal government.

[125] *Id.*

[126] U.S. Dep't of State, *Table I: Immigrant and Nonimmigrant Visas Issued at Foreign Service Posts Fiscal Years 2018–2022*, *in* Report of the Visa Office 2022 (2023), https://travel.state.gov/content/travel/en/legal/visa-law0/visa-statistics/annual-reports/report-of-the-visa-office-2022.html (reporting that the U.S. issued 6.8 million visas in 2022); *Exclusive: Security Gaps Found in Massive Visa Database*, ABC News (Mar. 31, 2016), https://abcnews.go.com/US/exclusive-security-gaps-found-massive-visa-database/story?id=38041051 ("the database contains more than 290 million passport-related records, 184 million visa records and 25 million records on U.S. citizens overseas.")

and travel authorization.[127] Such systems require meaningful investigation and oversight to ensure that individuals are not wrongfully denied services by biased, misused, or inaccurate AI. Yet an overly broad reading of the national security exemptions could remove these entire systems from OMB's purview because intelligence community agencies make some use of the systems.

OMB has significant latitude in how to interpret the broad "national security system" definition and can limit the reach of the exemption in full accordance with its statutory authority by adopting a use-case approach for AI systems. Under a use-case approach, AI systems would only be exempted from the Draft Guidance when they are used for a national security purpose or by a fully exempted intelligence community agency. For example, CCD's facial recognition system would be subject to the requirements of the Draft Guidance, but any use that the NSA makes of that facial recognition system would not be. A use case approach would also ensure that AI used for data analysis like Palantir would not be exempted from scrutiny when it is used by Health and Human Services or law enforcement,[128] even if it is also used by intelligence community agencies.[129]

The use-case definition should be paired with a requirement in the Draft Guidance that agencies must include dual-use systems in review and oversight. Dual-use systems are systems like CCD with a substantial non-national security purpose that are also used for some national security purposes. OMB should be explicit that such systems are covered by the Draft Guidance, subject to limited carveouts for elements of the system that are used for national security purposes. OMB should also be careful to note that just because a system collects information or intelligence that is ultimately used for national security does not mean that such a system falls under the national security system definition. Finally, OMB can limit abuse of the national security system exemption by requiring agencies to justify their exemptions. The onus should be on agencies to identify which systems are legitimately exempted and justify those exemptions to OMB with enough detail for OMB to provide meaningful oversight.

[127] CCD PIA at 10. ("Yes, the information in the CCD centralized database supports the implementation of the Department of State's visa, America citizens and passport programs. The information is required to make determinations for granting the various consular services being requested to validate applicant information and to provide centralized storage of information internally for use by posts, in addition to sharing and validating information with other government agencies.")

[128] Dave Nyczepir, *HHS makes Palantir data analytics platform available to all its agencies*, FedScoop (May 4, 2022), https://fedscoop.com/hhs-palantir-platform-bpa/; Mark Harris, *How Peter Thiel's Secretive Data Company Pushed Into Policing*, Wired (Aug. 9, 2017), https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/.

[129] Biddle, *supra* note 114.

CONCLUSION

EPIC welcomes OMB's efforts to ensure responsible AI development, procurement, and use throughout the federal government and applauds the OMB's inclusion of several key responsible AI provisions within the Draft Memorandum, including greater funding for AI risk management, a cross-agency AI use case inventory, procedures to decommission AI systems that fail to meet minimum safety standards, required training data cleaning and labeling, and additional procurement requirements when seeking AI systems. OMB can and should use its budgetary and oversight authorities to:

1. enforce agency compliance with the Draft Memorandum,
2. refine responsible AI provisions like AI impact assessments and AI use case inventory reporting to increase transparency and accountability for more types of AI systems,
3. increase agency data management practices through additional data minimization provisions and reinvigorated privacy impact assessment reporting requirements,
4. encourage AI adoption only where AI can serve as a curated tool to meet predefined agency needs, and
5. monitor national security systems and mandate AI risk management practices when they are used for other purposes covered by the Draft Memorandum.

We appreciate this opportunity to comment on OMB's Draft Memorandum and are willing to engage with OMB further on any of the issues raised within our comment, including universal AI evaluation requirements; coordination between AI impact assessments and privacy impact assessments; AI procurement reform; the risks of national security AI systems; and the need for greater transparency over government AI use. These recommendations relate closely to the goals of Executive Order 14410 and bolster the responsible AI provisions within OMB's Draft Memorandum to ensure that government development, procurement, and use of AI is safe, equitable, and trustworthy both now and long into the future.

Respectfully submitted,

/s/ John Davisson
John Davisson
Director of Litigation

/s/ Ben Winters
Ben Winters
Senior Counsel

<u>/s/ Jake Wiener</u>
Jake Wiener
Counsel

<u>/s/ Grant Fergusson</u>
Grant Fergusson
Equal Justice Works Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)