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

# MEMORANDUM

**To:** Executive Office of the President, Office of the Vice President, Office of Management and Budget
**From:** Electronic Privacy Information Center (EPIC)
**Date:** August 8, 2023
**Re:** **Integrating AI Requirements Into Section 208 Privacy Impact Assessments**

## I. Summary

This memorandum proposes that the White House Office of Management and Budget (OMB) update its Privacy Impact Assessment guidance under Section 208 of the E-Government Act of 2002[1] to include AI impact requirements. This updated OMB guidance would align with a May 4, 2023, statement from the White House announcing new initiatives for regulating how federal agencies use emerging AI tools, including new OMB policy guidance on the U.S. government's use of AI systems.[2] This memo proceeds as follows:

1. **AI Impacts are Privacy Impacts.** Section II of this memo explains that AI systems implicate the same privacy and data collection concerns at the core of Section 208. AI systems process and use personal data, so AI impact requirements are natural extensions of existing Privacy Impact Assessment requirements.

2. **Section 208 Encompasses the Procurement and Use of AI Systems.** Sections III and IV describe the contours of OMB's statutory authority, including current Privacy Impact Assessment requirements. Crucially, the "information technology" covered by Section 208 encompasses government AI systems, so the OMB is empowered to incorporate AI impact requirements within its Privacy Impact Assessment guidance.

3. **AI Impact Requirements Align with the Biden-Harris Administration's Broader Policy Goals.** Section V describes recent White House efforts to prioritize responsible AI development and use, highlighting ways in which AI impact requirements in Privacy Impact Assessments would mirror recommendations by the Biden-Harris Administration and the National Institute of Standards and Technology.

[1] 44 U.S.C. § 3501 note.
[2] Press Release, White House, FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety (May 4, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/.

4. **AI Impact Requirements Could Include Increased Reporting Requirements, Regular AI System Audits to Identify Privacy Risks, and Setting an Interagency Risk Tolerance Threshold to Manage Risky AI Systems.** Because the OMB has discretion over the exact content of Privacy Impact Assessments, Section VI proposes that the OMB clarify that Section 208 covers AI systems, incorporate NIST's recent AI Risk Management Framework, and pursue specific AI reporting and testing requirements when updating its Privacy Impact Assessment guidance under Section 208.

## II. Government AI Use Implicates Personal Privacy Concerns

The impacts of government AI use and those of government personal data collection are not wholly distinct. Rather, many forms of AI systems used by government—including automated decision-making systems—rely on personal data in ways that implicate the same privacy concerns as those protected by Privacy Impact Assessments under Section 208 of the E-Government Act.

First, many AI systems used by government agencies rely on datasets that include personally identifiable information.[3] To develop these AI systems—which encompass everything from eligibility screening algorithms[4] and fraud detection systems[5] to police face surveillance systems[6] and beyond—AI companies train their AI models on scores of personal data taken from commercial databases and public records. When government agencies use AI systems, they once again feed personal data from government or commercial databases into these systems to produce outputs like risk scores, eligibility determinations, and identification determinations—outputs that depend on the storage, processing, and use of personal data. In sum, AI systems are valuable because they can analyze and make predictions about people based on available data, not simply in their ability to automate a process.[7]

Second, the inferences, assumptions, and outputs that AI systems produce based on personal data may produce privacy harms *beyond* those attributable to the collection and dissemination of personal data.[8] When AI inferences are accurate, for example, they reveal private information about someone without their consent—information that may be misused by

[3] *See, e.g.*, EPIC, Screened & Scored in the District of Columbia 4–6, 8, 15, 20–25 (2022) [hereinafter "Screened & Scored Report"].

[4] *Id.* at 27–28.

[5] Screened & Scored Report at 24–25.

[6] *See Face Surveillance and Biometrics*, EPIC, https://epic.org/issues/surveillance-oversight/face-surveillance/ (last visited July 31, 2023).

[7] *See* Daniel Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 Nw. U. L. Rev. __ (forthcoming 2024).

[8] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793, 830–60 (2022) (typologizing different privacy harms); Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, Colum. Bus. Rev., 2019, at 22–28 (exploring overlap between data inferences and personal data).

those who can access it.[9] When AI inferences are wrong, they perpetuate errors in automated decisions that can restrict or undermine someone's access to services and opportunities like jobs or public benefits.[10] In either case, government agencies' use of AI inferences may weave historical biases about race, economic status, gender, and ability into life-altering government decisions.

Lastly, government AI systems may disclose personal information to third parties while processing data. Many government AI systems are not built internally, but rather procured from private vendors who develop and maintain the technologies.[11] The personal data that government agencies feed into these AI systems does not always stay within the government. Rather, AI vendors who maintain these systems often require that the personal data within an agency's possession be shared, combined with a vendor's proprietary data, or compared to public and commercial databases.[12] To use many AI systems, then, government agencies are *required* to disseminate personal and government data to private vendors.[13]

Ultimately, AI systems not only rely on the collection, use, and dissemination of personal data, but also perpetuate any errors or biases found in that data. Their procurement and use directly implicates the same privacy concerns at the core of Section 208 of the E-Government Act.[14]

## III. Section 208 of the E-Government Act of 2002 Requires Federal Agencies to Regularly Conduct Privacy Impact Assessments

In an effort to protect the privacy of personal information collected, maintained, and disseminated by federal agencies, Congress passed Section 208 of the E-Government Act in 2002.[15] Under Section 208(b)(1), every federal agency is required to conduct, review, and (if feasible) publish a Privacy Impact Assessment *before* it either (1) develops or procures information technology that collects, maintains, or disseminates personally identifiable information or (2) initiates a new collection of information.[16] These Privacy Impact Assessments must include, at minimum:

1. What information that will be collected;
2. The reason for collection;

[9] *See* Citron & Solove, *supra* note 8, at 831–33, 853 (discussing physical harm and lack of control); Wachter & Mittelstadt, *supra* note 8, at 12–19 (discussing automated methods for inferring intimate details about someone's identity and life).
[10] *See* Citron & Solove, *supra* note 8, at 817, 839–41 (discussing reputational harms caused by inaccuracies); Wachter & Mittelstadt, *supra* note 8, at 57 (discussing right to rectify inaccurate inferences).
[11] *See* Grant Fergusson, *Public Benefits, Private Vendors: How Private Companies Help Run Our Welfare Programs*, EPIC Blog (Jan. 26, 2023), https://epic.org/public-benefits-private-vendors-how-private-companies-help-run-our-welfare-programs/.
[12] *See id.*; Screened & Scored Report at 24–25 (describing one such arrangement with Thomson Reuters).
[13] *See* 44 U.S.C. § 3501 note at 208(b)(1)(A) (mandating Privacy Impact Assessments when an agency procures or uses information technology that disseminates personal information).
[14] *Id.* at 208(a).
[15] *Id.*
[16] *Id.* at 208(b)(1)(A)–(B).

3. The agency's intended use of the information;
4. Information about who the information will be shared with;
5. Information about the "notice or opportunities for consent [that] would be provided to individuals regarding what information is collected and how that information is shared;"
6. How the information will be secured; and
7. "[W]hether a system of records is being created under [the Privacy Act, 5 U.S.C. § 552a]."[17]

Although Section 208 dictates that Privacy Impact Assessments must include these minimum requirements, the OMB is also directed to provide guidance on the specific contours of Privacy Impact Assessments, including guidance requiring agencies to include other information within their Privacy Impact Assessments[18] and guidance that requires agencies to conduct Privacy Impact Assessments on already existing information systems or ongoing information collection efforts.[19]

## IV. The Text of Section 208 Permits the OMB to Incorporate AI Impact Requirements Within its Privacy Impact Assessment Guidance

Section 208 requires the OMB to issue guidance specifying the contents of Privacy Impact Assessments. But while Section 208's statutory language dictates *minimum* requirements for Privacy Impact Assessments, it grants the OMB broad authority to determine the *exact* contents of Privacy Impact Assessments. The OMB is directed to ensure that all Privacy Impact Assessments address a minimum set of questions about the information collection or technology listed above,[20] and the guidance must "ensure that a Privacy Impact Assessment is commensurate with the size of the information system being assessed, the sensitivity of the information that is in an identifiable form in that system, and the risk of harm form unauthorized release of that information."[21] Beyond these directions, the OMB is granted broad discretion over the substance and form of Privacy Impact Assessments.[22] The only strict limitation on the OMB's guidance relates to the timing of Privacy Impact Assessments: agencies can only be required to complete a Privacy Impact Assessment while (1) "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form,"[23] (2) "initiating a new collection of information,"[24] or (3) continuing to collect personally identifiable information or use existing information technology.[25]

The term, "information technology," used in Section 208 can encompass AI systems. The definition of the term in Section 208, as incorporated within OMB guidance, is borrowed from the Clinger-Cohen Act of 1996, which defines "information technology" as:

[17] *Id.* at 208(b)(2)(B).
[18] *Id.* at 208(b)(2)(B).
[19] *Id.* at 208(b)(3).
[20] *Id.* at 208(b)(2)(B)(ii).
[21] *Id.* at 208(b)(2)(B)(i).
[22] *Id.* at 208(b)(3).
[23] *Id.* at 208(b)(1)(A)(i).
[24] *Id.* at 208(b)(1)(A)(ii)
[25] *Id.* at 208(b)(3)(C).

> "[A]ny equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, movement, control, display, switching, interchange, transmission, or reception of data or information by [an] executive agency... [including] computers, ancillary equipment… software, firmware[,] and similar procedures, services (including support services), and related resources."[26]

No matter their form, the value of AI systems is in their use as tools to collect, maintain, process, analyze, or otherwise manipulate data. Most government AI systems operate as software, AI-enabled equipment, or AI services provided by vendors. Therefore, when an AI system is procured or used to process, store, or analyze personal data, it would fall cleanly within the definition of "information technology" covered under Section 208's Privacy Impact Assessment requirement.

A government agency's use of existing AI systems in new, distinct efforts to collect, store, process, or disseminate personal data can trigger Section 208's Privacy Impact Assessment requirement as well. As described above, agencies are required to complete a Privacy Impact Assessment not only when developing or procuring new information technology, but also when applying information technology to a new or ongoing collection of information. Although the term, "collection of information," is not defined in either Section 208 or the Clinger-Cohen Act, the inclusion of the phrase "ongoing collections of information"[27] within Section 208 suggests that a "collection of information" describes a distinct *effort* to collect data for a specific purpose, rather than each discrete *instance* of data collection. Further, the separation between Section 208(b)(1)(A)(i), which covers the development and procurement of information technology, and Section 208(b)(1)(A)(ii), which covers the initiation of new collections of information, suggests that a new collection of information need not be accompanied by the development or procurement of new information technology to trigger a Privacy Impact Assessment. In fact, Section 208(b)(3) grants the OMB discretion to impose Privacy Impact Assessments for existing information technologies *regardless* of how they are used. When agencies use existing AI systems to collect, store, process, use, or disseminate personal data, the OMB has clear statutory authority to require Privacy Impact Assessments.

Additionally, OMB guidance incorporating AI impact requirements within Privacy Impact Assessments can apply retroactively to AI systems already procured and used by federal agencies. Under Section 208(b)(3)(C) of the E-Government Act, the Director of the OMB is *mandated* to require that federal agencies "conduct Privacy Impact Assessments of existing information systems or ongoing collections of information that is in an identifiable form" if the Director determines that such an assessment would be appropriate.[28] Assuming that AI systems fall within Section 208's definition of "information technology" and new efforts to collect, store, process, or disseminate personal data using AI systems falls within the definition of "collection of information," then the Section 208(b)(3)(C) appears to permit the OMB to require agencies to

[26] 40 U.S.C. § 11101(6); *see also* OMB Circular No. A-130.

[27] Section 208(b)(3)(C).

[28] *Id.*

conduct new Privacy Impact Assessments—including AI impact requirements—for their existing AI systems and any ongoing collections of information that involve AI systems.

Finally, current OMB guidance around Privacy Impact Assessments is compatible with AI impact requirements. The most recent OMB guidance concerning Privacy Impact Assessments, OMB Circular No. A-130, defines "Privacy Impact Assessment" as encompassing determinations of the "risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system" as well as evaluations of "protections and alternate processes for handling information to mitigate potential privacy concerns."[29] The Privacy Impact Assessment should include both an analysis of these requirements and a "formal document detailing the process and the outcome of the analysis."[30]

Because the electronic information systems used to collect, use, process, and disseminate data within OMB Circular A-130 includes information technology under Section 208—and because information technology appears to include A.I. software and vendor services—existing OMB guidance is compatible with a requirement to assess the risks and effects of A.I. systems used by federal agencies to collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information. In fact, many of the specific requirements outlined in OMB Circular A-130 align with existing proposals for AI risk management frameworks. [31] Even the format of these Privacy Impact Assessments—including both a substantive analysis and an accounting of the process and outcome of the analysis—aligns with several reporting and transparency recommendations within existing AI risk management proposals.[32] Together, the text of Section 208 and the text of existing OMB guidance provides a strong basis for including AI impact requirements within Privacy Impact Assessments.

## V. Incorporating AI Impact Requirements within Privacy Impact Assessments Aligns with the Biden-Harris Administration's National AI Strategy

Over the past year, the Biden-Harris Administration has taken several steps to incorporate greater AI oversight into the federal government. For example, in October 2022, the White House Office of Science and Technology Policy (OSTP) published its Blueprint for an AI Bill of Rights, which established five guiding principles for AI development and use: safe and effective

[29] OMB Circular No. A-130 at 34. The term, "electronic information system," used in this OMB Circular is derived from the definition of "information system" in 44 U.S.C. § 3502, described as "a discrete set of information resources [including information technology] organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." 44 U.S.C. § 3502(8).

[30] *Id.*

[31] *See, e.g.*, NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) 7–9, 21–33 (2023) (discussing risk prioritization and proposing various steps to measure and manage AI risks) [hereinafter "NIST AI RMF"]; IEEE SA, Standard for the Procurement of Artificial Intelligence and Automated Decision Systems, P3119 (forthcoming 2024) (providing rubric for assessing different AI solutions throughout government procurement and use lifecycle); *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at 12–16, COM (2021) 206 final (Apr. 21, 2021) (summarizing AI risk assessment and reporting requirements under the E.U. Artificial Intelligence Act).

[32] *Id.*

systems; algorithmic discrimination protections; data privacy; notice and explanation; and human alternatives, consideration, and fallback.[33] For each principle, the OSTP included several AI assessment measures that could be incorporated within Privacy Impact Assessments as well. These measures include but are not limited to:

1. Pre-deployment testing to mitigate AI risks, including those that stem from the improper collection, use, or dissemination of personal data;[34]
2. Independent evaluations of each AI system's safety and effectiveness for its intended use(s), which the results of any evaluations made public whenever possible;[35]
3. Proactive equity assessments of AI systems, including assessments of the representativeness of data used to train the system;[36] and
4. Extending privacy protections for personal data to related inferences made by AI systems.[37]

In May 2023, the Biden-Harris Administration expanded its efforts to advance responsible AI use by announcing an updated roadmap for AI research and development, as well as an OSTP-led effort to identify national AI priorities.[38] As part of its updated roadmap, the Administration included several strategies for mitigating privacy harms within AI systems that mirror the privacy concerns at the core of Section 208's Privacy Impact Assessments. These strategies include but are not limited to:

1. Developing approaches to mitigate the ethical, legal, and social risks of AI systems, including by advancing AI explainability efforts and investing in privacy-enhancing technologies like homomorphic encryption, differential privacy, and secure multiparty computation;[39]
2. Developing shared public datasets to train and test AI systems without revealing confidential or otherwise personally identifiable information;[40]
3. Developing standards for auditing and monitoring AI systems, including audits for privacy risks;[41] and

[33] OSTP, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People 5–7 (2022).
[34] *Id.* at 5, 15–16.
[35] *Id.* at 5, 15, 20.
[36] *Id.* at 5, 23, 26.
[37] *Id.* at 6, 30.
[38] Press Release, White House, FACT SHEET: Biden-Harris Administration Takes New Steps to Advance Responsible Artificial Intelligence Research, Development, and Deployment (May 23, 2023), https://www.whitehouse.gov/ostp/news-updates/2023/05/23/fact-sheet-biden-harris-administration-takes-new-steps-to-advance-responsible-artificial-intelligence-research-development-and-deployment/.
[39] Select Comm. on A.I., Nat'l Sci. & Tech. Council, National Artificial Intelligence Research and Development Strategic Plan 2023 Update vii, 12–14 (2023).
[40] *Id.* at 18–20.
[41] *Id.* at 26.

4. When needed, providing private individuals or entities with access to data through secure government platforms.[42]

Several of these AI risk management strategies were reflected in the White House's July 2023 announcement that it had secured voluntary AI commitments from seven leading AI companies, including commitments to independently test AI systems for cybersecurity and privacy risks and publicly report the capabilities, limitations, and proper uses of AI systems.[43] However, more can be done to extend the Biden-Harris Administration's efforts to government AI use—and the OMB is well-positioned to implement the Biden-Harris Administration's national AI priorities.

Many of the AI oversight policies championed by the Biden-Harris Administration already mirror existing OMB guidance. Under OMB Circular A-130, for example, agencies are required to, *inter alia*, (1) develop a plan for replacing or retiring information systems that can be appropriately secured against privacy risks; (2) "regularly review and address risk regarding process, people, and technology; (3) "limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of [personally identifiable information] to that which is legally authorized, relevant, and reasonably deemed necessary;" and (4) "protect information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information."[44] While some of the Administration's AI policy priorities will require additional government efforts, several policy provisions concerning the testing, evaluation, and reporting of AI systems can be incorporated into Privacy Impact Assessments under Section 208. Incorporating AI impact requirements within Privacy Impact Assessments would not extend OMB guidance beyond what Section 208 allows, but rather align OMB guidance with broader governmental priorities around privacy and AI systems.

## VI. AI Impact Requirements Could Include Increased Reporting Requirements, Regular AI System Audits to Identify Privacy Risks, and Setting an Interagency Risk Tolerance Threshold to Manage Risky AI Systems

The text of Section 208 empowers the OMB to incorporate AI impact requirements into its guidance surrounding Privacy Impact Assessments. However, the OMB has discretion to determine the exact shape and extent of these requirements. This section suggests three steps that OMB could take to incorporate AI impact requirements within the OMB's Privacy Impact Assessment guidance.

First, OMB should issue explicit guidance to agencies clarifying that existing Privacy Impact Assessment requirements extend to the procurement and use of AI systems. Under

[42] *Id.* at 19.

[43] Press Release, White House, FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

[44] OMB Circular No. A-130 at 6, 17–18.

Section 208 and OMB Circular A-130, an agency is required to conduct a Privacy Impact Assessment whenever it "develops, procures, or uses information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of [personally identifiable information]."[45] These Privacy Impact Assessments must analyze how personal data is handled, determine the privacy risks associated with an information system or activity, evaluate ways to mitigate privacy risks, and detail the process and outcomes of each analysis.[46] Moreover, each Privacy Impact Assessment is meant to be "living document that agencies are required to update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology."[47] By clearly stating that the procurement and use of AI systems that collect, process, use, or disseminate personal data falls within the scope of an agency's Privacy Impact Assessment obligations under Section 208, the OMB can capture several AI impact requirements automatically, such as analyses of how an AI system uses personal data, determinations of the privacy risks associated with an AI system, and evaluations of the ways to mitigate an AI system's privacy risks.

Second, OMB could incorporate NIST guidance on AI risk management into its Privacy Impact Assessment guidance. OMB Circular A-130 already leverages NIST standards like the Federal Information Processing Standards (FIPS) and NIST Special Publications from the 500, 800, and 1800 series.[48] By incorporating assessment, documentation, and reporting recommendations from NIST's AI Risk Management Framework (AI RMF)[49] into its Privacy Impact Assessment guidance, for example, OMB can rapidly incorporate specific AI impact requirements into Privacy Impact Assessments without extending beyond its statutory authority under Section 208. Examples of NIST AI RMF recommendations that could be incorporated within Privacy Impact Assessments include but are not limited to:

- Establishing processes and procedures for decommissioning AI systems safely and in a manner that does not increase risks or decrease the agency's trustworthiness;[50]
- Documenting information about an AI system's knowledge limits and how system output may be utilized and overseen by humans;[51]
- Documenting AI training and testing datasets, evaluation metrics, and other testing procedures;[52]
- Testing AI systems for validity and reliability—and documenting AI system limitations—before they are deployed;[53]

[45] *Id.* at 74–75 (Appendix II).
[46] *Id.*
[47] *Id.*
[48] *Id.* at 6.
[49] NIST AI RMF at 21–34.
[50] *Id.* at 23.
[51] *Id.* at 26.
[52] *Id.* at 29.
[53] *Id.*

- Regularly evaluating AI systems for privacy and safety risks based on a predetermined agency risk tolerance;[54]
- Incorporating resource constraints into AI system management determinations such that agencies do not procure or use AI systems they cannot adequately oversee;[55] and
- Communicating AI privacy incidents and errors to relevant authorities and affected communities.[56]

NIST's AI RMF is the result of a Congressional mandate, several years of careful consideration, and consultations with a wide range of stakeholders. The OMB can and should incorporate key recommendations from the AI RMF into its Privacy Impact Assessment guidance to align its efforts with existing standards and broader government efforts to oversee AI use.

Third, in line with both White House and NIST guidance on AI, the OMB could mandate specific AI impact requirements within Privacy Impact Assessments that are tailored to the statutory contours of Section 208 of the E-Government Act. At minimum, EPIC recommends incorporating three such requirements:

1. Reporting additional information about the procurement and use of AI systems, including:
    a. The intended purpose and proposed use of an AI system;
    b. What decision(s) the AI system is making or supporting;
    c. The role that the AI system plays in making the decision;
    d. The AI system's intended benefits and research supporting the benefits;
    e. The AI system's capabilities, including capabilities outside the scope of its intended use, as well as uses for which it is not appropriate;
    f. An assessment of the relative benefits, costs, and risks to the public given the system's purpose, capabilities, and probable use cases;
    g. The inputs and logic of the AI system;
    h. The data or inputs used to train and test the AI system;
    i. Any testing and evaluation methods the agency intends to use, including the frequency of testing and any results or findings produced.

2. Conducting regular AI testing and evaluation processes to identify any errors, biases, vulnerabilities, or privacy risks within AI systems, including, where applicable, evaluations of the representativeness of training data, the validity of AI system outputs across different use contexts, and any changes in AI system outputs that may indicate a degradation in the accuracy or reliability of the AI system.

3. Setting an interagency privacy risk tolerance threshold based on the NIST AI RMF and updated to reflect ongoing agency testing and evaluation of AI systems, such that

[54] *See id.* at 30.
[55] *Id.* at 32.
[56] *Id.* at 33.

agencies would be prohibited from using AI systems that exhibit an excessive level of risk to the data security or privacy of individuals. EPIC has previously identified at least two AI systems—emotion recognition systems and one-to-many facial recognition systems—as exhibiting excessive levels of risk to individuals' privacy.[57]

## VII. Conclusion

Section 208 is one of only one of many tools necessary to ensure responsible and effective government use of AI systems. AI impact assessments and reporting requirements are an effective way to mitigate AI risks, but they are not a full regulatory solution to the ongoing and emerging risks that AI systems bring. Formal restrictions, federal procurement guidelines, and explicit prohibitions on high-risk AI systems and use cases are also necessary to ensure the AI systems that federal agencies procure and use are trustworthy and effective.

[57] *See, e.g.*, EPIC, Comments on FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security 98–108, 87 Fed. Reg. 51273 (Nov. 21, 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.