epic.org

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

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

U.S. DEPARTMENT OF STATE

Notice of a Modified System of Records, Department of State

Passport Services Records, State-26

91 Fed. Reg. 66,906 | DOS–2026–1156

November 23, 2026

The Electronic Privacy Information Center (EPIC) submits these comments in response to the System of Records Notice for the Passport Services Records (the Notice) published in the Federal Register by the Department of State (State) on October 23, 2026.[1] EPIC is a public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[2]

The Notice should be promptly withdrawn and its proposed routine uses abandoned. Through the Notice, the State attempts to unlawfully reconfigure the Passport Services Records (PSR)[3] system, what was meant to be a passport adjudication and benefits eligibility verification system, into an entirely new direction as a voter eligibility tool. But the State cannot lawfully pursue this course of action and its Notice to that end is deficient.

The Notice fails for at least two reasons. First, proposed routine use (w) fails the requirements of the Privacy Act. The proposed routine use would allow the State Department to share sensitive data held in the PSR to various government agencies and some unspecified non-profit organizations for purposes of "voter eligibility."[4] But this routine use fails to meet the compatibility and specificity that the Privacy Act requires. Second, and more broadly, the Notice attempts to retroactively change the purpose of the PSR by adding that the "system maintains information that is used to establish the U.S. nationality and identity of persons for a variety of legal purposes including, but not limited to … *voter eligibility*."[5] But none of the legal authorities that the Notice relies on legitimates this after-the-fact repurposing of the PSR to conduct voter verification. Accordingly, the State should withdraw the Notice.

---

[1] 91 Fed. Reg. 66906 (Oct. 23, 2026), https://www.federalregister.gov/documents/2026/10/23/2026-21695/privacy-act-of-1974-system-of-records.
[2] *See About Us*, EPIC.org, https://epic.org/about/.
[3] The Notice renames the "Passport Records" system, 80 Fed. Reg. 15653, as the "Passport Services Records" system. EPIC uses "Passport Services Records" system to refer to the existing SORN and new SORN for the sake of convenience.
[4] 91 Fed. Reg. at 66909.
[5] *Id.* at 66907 (emphasis added).

I. The proposed routine use (w) fails to satisfy the Privacy Act.

The Notice purports to add routine use (w), which would allow records to be shared with "[va]arious entities including, but not limited to, Federal, state, territorial, tribal, and local government agencies, and non-profit organizations, utilizing federal government verification platforms, for the purpose of verifying the identity or citizenship for users accessing government websites and applications, voter eligibility, and other government services."[6] But this routine use does not comport with the original purpose of the collection and fails the Privacy Acts compatibility and specificity requirements.

a. Voter eligibility is not compatible with the original purpose of the PSR.

The routine use exception permits disclosure only "for a purpose which is compatible with the purpose for which [the record] was collected."[7] Determining "compatibility" requires "a dual inquiry into the purpose for the collection of the record in the specific case and the purpose of the disclosure."[8] Once the purposes of the collection and disclosure are identified, there must be more than a mere "relevance" of the disclosure's objective to the collection's aim.[9] Instead, there must be "a concrete relationship or similarity, some meaningful degree of convergence" between the original and new purposes."[10] The D.C. Circuit, following Office of Management and Budget guidance, has looked to whether the new use is functionally equivalent to the original purpose or necessary and proper to it.[11] The State's stated aim of "voter eligibility" fails to fulfill that standard.

Before the proposed Notice, the PSR was a system that was used to establish the identity and nationality of persons to adjudicate passport applications, verify eligibility for social security benefits and employee applications, and for certain law enforcement purposes.[12] Under the PSR, the State collected and managed information to administer passport records such as via the Passport Information Electronic Records Systems (PIERS).[13] The PSR was not a comprehensive database used to verify voter eligibility and such a use is not "compatible with the purpose for which it was collected."[14]

---

[6] *Id.* at 6609.
[7] 5 U.S.C. §§ 552a(a)(7), (b)(3).
[8] *Britt v. Naval Investigative Service*, 886 F.2d 544, 584-49 (3d Cir. 1989).
[9] *Id.* at 549.
[10] *Id.* at 549–50 (citing Mazaleski v. Treusdell, 562 F.2d 701, 713 n. 31 (D.C.Cir. 1977)) (other citation omitted).
[11] *U.S. Postal Service v. National Ass'n of Letter Carriers*, 9 F.3d 138 (D.C. Cir. 1993) (citing 40 Fed. Reg. 28,948, 28,953 (July 9, 1975)).
[12] 80 Fed. Reg. 15653, 15654 (2015).
[13] State, *Privacy Impact Assessment for the Passport Information Electronic Records System (PIERS)* (2020), https://www.state.gov/wp-content/uploads/2020/11/Passport-Information-Electronic-Records-System-PIERS-PIA.pdf.
[14] 5 U.S.C. §§ 552a(a)(7), (b)(3)

This should come as no surprise as the PSR is unfit for voter eligibility verification. Passport eligibility and voter-eligibility determinations turn on entirely different legal qualifications. An individual may be denied a passport for reasons that would not impact voting-eligibility. For example, a person might be denied a passport for certain drug-trafficking convictions[15] as well as certain child-support and tax debts.[16] But that same person would nonetheless still be fully eligible to vote. The reverse may also occur: a person whose state has removed voting rights after a felony conviction may still hold a valid passport. Whether someone is eligible to vote is determined by state-specific criteria and information collected for purposes of a passport does not have any bearing on that question. No one needs a passport to vote, and a missing passport record says nothing about voting-eligibility.

b. The Notice has numerous other Privacy Act deficiencies.

The Notice's proposed routine use is afflicted with numerous other Privacy Act deficiencies.

First, proposed routine use (w) is too vague for "interested persons" to provide fully informed "written data, views, or arguments."[17] The routine use authorizes disclosure to "various entities including, but not limited to federal, state, territorial, tribal, and local governments and "non-profit organizations," for "other governmental services" beyond identity, citizenship, and voter eligibility.[18] The Notice does not detail what these governmental services might be. And taking such language at face value would give the State boundless authority to share data for any government service. But such a proposition is completely at odds with the Privacy Act's mandate to limit disclosure. In addition, the routine use contemplates disclosure to unidentified "non-profit organizations," but no details are given as to what type of non-profits the State would disclose information to. In fact, no information is provided in the Notice as to why these non-profits would get potential access to the records of millions of individuals who have applied for a passport. Such an omission is especially egregious considering the sensitive nature of the records at issue. Besides the passports themselves, the PSR also contains, passport application materials which include among other things copies of photo ID such as driver's licenses and birth certificates.[19]

Second, the proposed routine use creates significant security risks that the Notice's lack of detail only makes more concerning. Disclosure of such sensitive data to non-profit organizations without any enumeration of how the data will be secured is a direct violation of the duty to "establish appropriate administrative, technical, physical safeguards to insure the security and confidentiality of records."[20] The allusions to "cyber security awareness training" do not suffice, especially considering the Federal government's dubious adherence to cyber security

[15] 22 U.S.C. § 2714.
[16] 22 U.S.C. § 2714a.
[17] 5 U.S.C. § 552a(e)(7).
[18] 91 Fed. Reg. at 66907.
[19] *See* Dep. Of State, *Apply for your Adult Passport* (accessed Nov. 22, 2026), https://travel.state.gov/en/passports/apply/adults.html#accordion-e38fdea780-item-9a65575094.
[20] 5 U.S.C. § 552a(e)(10).

guidelines,[21] and the ability of contractors to access the records from "non-Department owned information technology."[22] The spate of recent data breaches[23] that the federal government has experienced only further emphasize the State's dereliction of duty in this Notice.

Third, the sharing of passport records for citizenship screening without any safeguards for accuracy is inconsistent with the Privacy Act's accuracy requirements. The Privacy Act mandates that the agency must make "reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes."[24] Routine use (w) would permit use of the record for voter eligibility without any limits to confirming matches or barring adverse conclusions from non-matches. Over the past months, other federal citizenship-verification tools have reported high numbers of misidentified eligible citizens.[25] Routine use (w), without these limits, does not reflect reasonable efforts at accuracy required by the Privacy Act.

II. The Notice exceeds the State's statutory authority.

The State's attempts to introduce "voter eligibility" as a purpose of the PSR fail because it lacks the requisite statutory authority. Federal administrative agencies are "creatures of statute"[26] and only possess authority that Congress has provided.[27] Congress has never conferred the authority the State now attempts to claim: the ability to verify voters.

No statute listed in the Notice's "Authority for Maintenance of the System" is meant to regulate voter eligibility. Instead, the statutes cover nationality and passport laws,[28] criminal passport-fraud laws,[29] and tax reporting.[30] As the State cannot identify any statutory authority to assume a voter-verification role, routine use (w) exceeds the State's statutory authority. Nor do the executive orders the Notice cites supply the authority the State seeks. To begin with, the Notice cites no executive order for voter verification. And even if the State did, such an order

---

[21] *See* GAO-27-108661, *Cybersecurity: Agencies Need to Fully Address Federal Guidance As They Refine Zero Trust Architecture* (Nov. 18, 2026) (finding 17 agencies, including the State, failing to address guidance for verifying attempts to access system and services).
[22] 91 Fed. Reg. at 66909.
[23] AP, *FBI Investigating Apparent Hack of Its Key National Criminal Justice Database* (Nov. 21, 2026), https://www.pbs.org/newshour/politics/ap-source-fbi-investigating-apparent-hack-of-its-key-national-criminal-justice-database; Jenna McLaughlin et al, *FBI Investigating Massive Data Breach of the Bureau's Job Portal*, NPR (Sep. 30, 2026), https://www.npr.org/2026/09/30/nx-s1-5985084/fbi-investigating-massive-data-breach-of-the-bureaus-job-portal.
[24] 5 U.S.C. § 552a(e)(6)
[25] Jen Fifield et al, *A Federal Tool to Check Voter Citizenship Keeps Making Mistakes*, Texas Tribune (Feb. 13, 2026), https://www.texastribune.org/2026/02/13/save-voter-citizenship-tool-mistakes-confusion/.
[26] *Nat'l Fed'n of Indep. Bus. V. Dep't of Lab*., 595 U.S. 109, 117 (2022).
[27] *Louisiana Public Service Commission v. FCC*, 476 U.S. 355, 374 (1986),
[28] 8 U.S.C. §§ 1104, 1185, 1401–1504; 22 U.S.C. §§ 211a–218, 2651a, 2705, 2714, 2714a)
[29] 18 U.S.C. §§ 911, 1001, 1541–1546.
[30] 26 U.S.C. § 6039E.

would have no effect. The President's power "must stem either from an act of Congress or from the Constitution itself."[31] Here, the State cannot point to either.

Congress's sole express authorization to share passport application data with another federal agency is unrelated to voter eligibility. 26 U.S.C. § 6039E only requires passport applicants to provide certain information and directs the State to transmit it to the Treasury Department for tax compliance, as routine use (c) acknowledges. Courts presume that Congress acts deliberately when it addresses a subject expressly in one place and not in another.[32] In § 6039E, Congress specified what information would be shared, with which agency, and for what purpose. It enacted no comparable statute for voter eligibility. The absence of any such provision, when Congress knew how to write one, indicates that it has not authorized this use.

When Congress has addressed voter-registration verification, it has chosen other means. The Constitution gives the states the power to set voter qualifications and gives Congress the power to regulate the times, places, and manner of federal elections.[33] Congress has exercised that power in the Help America Vote Act, which requires each state's computerized voter registration list to be checked against state motor vehicle records and against Social Security Administration data.[34] It also exercised it in the National Voter Registration Act, which assigns enforcement power to the Election Assistance Commission and the Department of Justice.[35] Neither gives the State Department any role or mentions passport records. The State cannot fill that gap on its own via this Notice.

III. Conclusion

For the above reasons, the State Department should promptly withdraw its Notice and terminate any related modifications still under consideration. If you require any additional information please contact John Davisson, EPIC Director of Litigation, at davisson@epic.org.

Respectfully submitted,

Electronic Privacy Information Center (EPIC)

[31] *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 585 (1952).
[32] *Cf. Russello v. United States*, 464 U.S. 16, 23 (1983).
[33] U.S. Const. art. I, § 4, cl. 1; *see Arizona v. Inter Tribal Council of Arizona, Inc.*, 570 U.S. 1, 16–17 (2013).
[34] 52 U.S.C. § 21083(a)(5)
[35] 52 U.S.C. § 20501 et seq.