

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
AND 13 ORGANIZATIONS

to the

U.S. SOCIAL SECURITY ADMINISTRATION

System of Records Notice, Master Files of Social Security Number (SSN) Holders and SSN Applications (60-0058)

90 Fed. Reg. 50,879 | SSA-2025-0225

December 12, 2025

The Electronic Privacy Information Center (EPIC) and the undersigned organizations submit these comments in response to the System of Records Notice (“SORN” or “the Notice”) for the modification of an existing systems of records titled “Master Files of Social Security Number (SSN) Holders and SSN Applications (60-0058)” published in the Federal Register by the Social Security Administration on November 12, 2025.¹ 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.

Over the past eight months, the Department of Homeland Security (DHS) and Social Security Administration (SSA) have effected radical changes to the Systematic Alien Verification for Entitlements (SAVE) system in defiance of long-established safeguards on how the system can be used, what types of records it incorporates, and whose information can be accessed. A tool once used to facilitate the provision of public benefits now serves as a jerry-rigged national citizenship database: an error-ridden system with vast quantities of sensitive personal information from Americans and noncitizens alike. Equally concerning, the system—newly linked to sensitive records from the Master Files of Social Security Number Holders and SSN Applications (Master Files) system—can now be queried in bulk by states looking to kick voters off of their rolls. These changes have been made with the complicity of SSA in clear violation of federal law, without public or Congressional input, and against stern warnings issued in recent years by the very agencies involved in the system’s overhaul.

Half a year after these changes began, SSA now comes before the public to seek retroactive authority for its role in these sweeping violations of privacy and voting rights through the instant Notice. But the sensitive personal information of tens of millions cannot be so casually abused under federal law: the Privacy Act demands more of federal agencies. First, the Notice does nothing to legitimize the wrongful disclosure of personal information that SSA has carried out over the past year; the Privacy Act is clear that agencies must solicit public comment on proposed uses of personal information before they act on them. Second, the routine uses set out in the Notice fall far short of the compatibility and specificity that the Privacy Act requires

¹ 90 Fed. Reg. 50879, 50879 (Nov. 12, 2025) (“2025 Revised SSA SORN”).

and suggest that the SSA is contributing to the creation of unlawful national data banks. Third, SSA violates not only the Privacy Act, but the Social Security Act and its own policies by disclosing its records to DHS and other state and federal government agencies through SAVE. Finally, the agency’s failure to identify or disclose any Computer Matching Agreements applicable to the overhauled SAVE system represents an independent violation of the Privacy Act.

Accordingly, SSA should promptly withdraw its Notice, immediately suspend the disclosure of personal records to DHS for citizenship and immigration purposes, and take the steps necessary to ensure that DHS and downstream SAVE users delete all personal records and derived data they wrongfully obtained as a consequence of such disclosures to date.

I. SSA’s after-the-fact publication of a modified system of records notice cannot legitimize its participation in the radical restructuring of the SAVE system.

We object to SSA’s failure both to provide a meaningful opportunity to be heard on the proposed Notice and to conduct a meaningful review of public comments prior to the agency’s addition of a new routine use to facilitate DHS’s overhaul of the SAVE system.² Having already violated its statutory notice obligations, SSA now seeks to absolve itself of its unlawful actions through the belated publication of a System of Records Notice. This it cannot do, particularly through a Notice that fails to meet the substantive requirements of the Privacy Act.

The Privacy Act requires an agency to, “at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.”³ Paragraph (4)(D) of the subsection refers to “each routine use of the records contained in the system, including the categories of users and purpose of such use.”⁴ Further, agencies cannot “use a new or significantly modified routine use as the basis for a disclosure fewer than 30 days following Federal Register publication.”⁵

The agency failed to provide adequate notice before disclosing SSA-held personal data to DHS for the purposes of expanding the SAVE system. The U.S. Citizenship and Immigration Services (USCIS) last published a revised Notice for the SAVE system in 2020.⁶ SSA last published a revised Notice to modify the “Master Files of Society Security Number (SSN) Holders and SSN Applications (60-0058)” system of records in February 2025.⁷ On April 22, 2025, DHS, USCIS, and the Department of Government Efficiency (DOGE) announced that they would “overhaul” the SAVE system to enable “mass status checks” and the integration of

² See 90 Fed. Reg. 48948, 48948 (Oct. 31, 2025) (“2025 DHS SAVE SORN”).

³ 5 U.S.C. § 552a(e)(11).

⁴ *Id.* at § 552a(e)(4)(D).

⁵ Off. of Mgmt. & Budget Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 7 (2016), <https://perma.cc/N9QK-SDLE> (“OMB Circular No. A-108”).

⁶ 85 Fed. Reg. 31798, 31798 (May 27, 2020).

⁷ 90 Fed. Reg. 10025, 10025 (Feb. 20, 2025).

“criminal records, immigration timelines, and addresses.”⁸ On May 15, 2025, SSA, DHS, and USCIS agreed to an information-sharing arrangement between the agencies whereby SSA would share SSA records regarding citizenship or immigration status, including full or partial social security numbers.⁹ The agreement specified that the overhauled SAVE system would match data to SSA’s Master Files system of records, which at the time did not list data sharing to the DHS and USCIS for citizenship verification as a routine use.¹⁰ On May 22, 2025, USCIS announced that it had dramatically altered the SAVE program, making it now a single source “for verifying immigration status and U.S. citizenship nationwide.”¹¹ The agency further stated that it would “continue to improve and add more capability and functionality to SAVE.”¹² The USCIS also updated its SAVE “fact sheet” to reflect significant changes to the overhauled SAVE system in August 2025.¹³

SSA’s after-the-fact Notice is insufficient: the agency is already enabling SAVE system’s unlawful access to citizenship and immigration information—and has been since May 2025. Despite the Notice indicating that new routine uses will be effective December 12, 2025, DHS and other agencies are actively using the overhauled SAVE system to access SSA data and encouraging states to use the tool to run citizenship checks.¹⁴ States like Texas and Louisiana have already used the SAVE system to identify purported noncitizens registered to vote.¹⁵ This cart-before-the-horse linking of SSA data to the overhauled SAVE system not only violates SSA’s public notice obligations; it also violates the agency’s notice obligations to Congress and the Office of Management and Budget (OMB).¹⁶ Members of Congress were not informed prior to the expansion of the SAVE system and rightly criticized the lack of transparency around the use of the system.¹⁷ The Notice does not mention the SAVE system despite the new routine use being clearly used in connection to DHS’s overhauled SAVE system for immigration and citizenship verification. Additionally, SSA’s data sharing agreement with DHS and USCIS was released through a FOIA request months after the agreement went into effect. The agency’s covert actions demonstrate an egregious undermining of public and congressional accountability.

⁸ Press Release, *DHS, USCIS, DOGE Overhaul Systematic Alien Verification for Entitlements Database*, DHS, (Apr. 22, 2025), <https://perma.cc/Y8A5-YX3M>.

⁹ Letter Agreement Providing for Information Sharing Between DHS, USCIS, and SSA Regarding Citizenship (May 12, 2025), <https://perma.cc/ZTB9-GJ8F> (“DHS-SSA SAVE Agreement”).

¹⁰ *Id.* at 4; *see* 90 Fed. Reg. 10025, 10025 (Feb. 20, 2025).

¹¹ Press Release, *USCIS Deploys Common Sense Tools to Verify Voters*, USCIS (May 22, 2025), <https://perma.cc/HBZ5-RW2E>.

¹² *Id.*

¹³ *Voter Registration and Voter list Maintenance Fact Sheet*, USCIS (last updated Aug. 27, 2025), <https://perma.cc/PP4H-T7CK>.

¹⁴ *See* Jude Joffe-Block & Miles Parks, *33 Million Voters Have Been Run Through a Trump Administration Citizenship Check*, NPR (Sep. 11, 2025), <https://perma.cc/QWL3-DCVR>.

¹⁵ *See* Press Release, *Texas Completes Citizenship Verifications in Save Database*, TX Sec. of State (Oct. 20, 2025), <https://www.sos.state.tx.us/about/newsreleases/2025/102025.shtml>; Wesley Muller, *Louisiana Election Investigation Finds 79 Noncitizens Have Voted Since 1980s*, Louisiana Illuminator (Sep. 4, 2025), <https://lailuminator.com/2025/09/04/louisiana-election-investigation-finds-79-noncitizens-have-voted-since-1980s/>.

¹⁶ 5 U.S.C. § 552a(r).

¹⁷ *See e.g.*, Letter from Senators Alex Padilla, Ranking Member of the Senate Rules and Admin Comm., Gary Peters, Ranking Member of the Senate Homeland Sec. and Gov’t Aff. Comm., and Jeff Merkley, to Kristi Noem, Sec., DHS (July 15, 2025), <https://perma.cc/3KD2-FCNQ>.

The Privacy Act sets forth specific review, reporting, and publication requirements prior to the modification of a system of records which this belated Notice fails to meet. Even if the Notice were otherwise adequate—and it is not—a Notice issued long after SSA undertook major modifications to the Master Files system cannot cure the agency’s unlawful (and ongoing) use of that modified system. By ignoring mandatory safeguards set forth in the Privacy Act, SSA is skirting its accountability and transparency obligations and further undermining public trust.

II. The two new routine uses to disclose citizenship and immigration information and expand Do Not Pay set out in the modified Notice fail to satisfy the Privacy Act.

To align with the Trump administration’s various executive orders and stated intention to identify (virtually nonexistent) noncitizen voting,¹⁸ SSA is allowing the SAVE system to query Social Security data to verify the citizenship status of registered voters.¹⁹ The Notice, completed months after SSA began disclosing personal records in connection with the SAVE system, attempts to paper over SSA’s Privacy Act violations by asserting a new legal basis to allow for the unlawful consolidation, use, and disclosure of personal information. This attempt fails.

By providing access to Social Security data, SSA is complicit in DHS’s transformation of SAVE from a limited-purpose tool into a system that incorporates sensitive personal data about virtually all Americans and noncitizens in the United States. New record sources for SAVE include SSA’s Numerical Identification System (Numident),²⁰ which maintains records from SSA’s Master Files of the Social Security Holders and SSN Applications.²¹ These records contain each individual who has applied for a Social Security Number since 1936; the data categories include Social Security numbers, names, dates of birth, both parents’ names, sex identification, and other information processed in applications for Social Security numbers.²² In other words, the SAVE system has been radically, and unlawfully, expanded to access sensitive records of over 300 million individuals in the U.S.²³

The Notice purports to establish two additional routine uses. First, it attempts to create Routine Use 49, which would allow SSA to disclose to DHS records “regarding the citizenship and immigration status, lawful or unlawful, of any individual pursuant to 8 U.S.C. 1373(a).”²⁴ Second, the Notice also proposes Routine Use 50, which allows SSA to disclose records to the U.S. Department of the Treasury for use in that agency’s Do Not Pay Working System.²⁵ For the

¹⁸ See Miles Parks, *Despite Grand Claims, a New Report Shows Noncitizen Voting Hasn't Materialized*, NPR (July 30, 2025), <https://www.npr.org/2025/07/30/nx-s1-5462836/noncitizen-voting-trump-ceir-review>; Stuart A. Thompson, *No, Noncitizens Are Not Voting in Droves*, NY Times (Oct. 28, 2024), <https://www.nytimes.com/2024/10/28/technology/noncitizen-voting-election.html>.

¹⁹ DHS, *Privacy Impact Assessment for the Systematic Alien Verification for Entitlements “SAVE” Program*, at 8 (Oct. 31, 2025), <https://perma.cc/Q3AX-KQS7> (“2025 DHS SAVE PIA”).

²⁰ *Id.*

²¹ *Frequently Asked Questions: Numerical Identification (NUMIDENT) Files*, Appendix, National Archives (last updated July 27, 2022), <https://perma.cc/6NWK-5B2Z>.

²² *Id.*

²³ See Geoff Brumfiel, *Whistleblower Says Trump Officials Copied Millions of Social Security Numbers*, OPB (Aug. 26, 2025), <https://www.opb.org/article/2025/08/26/whistleblower-says-doge-put-social-security-numbers-at-risk/>; Carolyn Puckett, *The Story of the Social Security Number*, SSA (July 2009), <https://perma.cc/QCR7-64DE>.

²⁴ 2025 Revised SSA SORN at 50883.

²⁵ *Id.*

reasons below, these new “routine uses” fail to satisfy the Privacy Act’s requirements, making disclosure of SSA data unlawful.

a. The disclosure of citizenship and immigration status is incompatible with the purpose for which SSA records were originally collected.

Routine Use 49—allowing disclosure “[t]o DHS, [of] information regarding the citizenship and immigration status, lawful or unlawful, of any individual pursuant to 8 U.S.C. 1373(a)”—is not a lawful basis for the use and disclosure of Social Security data through the SAVE system. Among the exceptions to the Privacy Act’s general prohibition on the disclosure of personal records are “routine use” disclosures, i.e., those made “for a purpose which is compatible with the purpose for which [a record] was collected.”²⁶ 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.”²⁷ 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.²⁸ Instead, “[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency’s purpose in gathering the information and in its disclosure.”²⁹

SSA fails to satisfy the Privacy Act’s requirements by failing to both (1) provide a purpose; and (2) show that the actual purpose for which the data is already being used for—verifying citizenship and immigration status of an individual through SAVE³⁰—is compatible with the purpose for which the data was originally collected. On its face, Routine Use 49 fails to provide a purpose for disclosure, much less a valid one under the Privacy Act; rather, it only provides notice that the citizenship and immigration information will be disclosed to DHS.³¹ Thus, this Notice fails the compatibility test for the Privacy Act at step one, as SSA has failed to actually identify the purpose for such disclosures.

But, to the extent that SSA understands the purpose for disclosure to be the verification of individuals’ citizenship and immigration status (as DHS provided in its SORN on the SAVE system),³² such a disclosure is incompatible with the purpose for which the SSA records were originally collected. The Master Files that SAVE accesses (maintained through Numident) were (and are) created or collected for the purpose of tracking the earnings of U.S. workers and determining benefit entitlements as established under the Social Security Act of 1935.³³ To administer the Social Security laws, the Social Security Number (SSN) was created in 1936.³⁴ Since its advent, the public was concerned about privacy and confidentiality of data collected in the process of applying for a Social Security number.³⁵ To protect the sensitive data collected by

²⁶ See 5 U.S.C. §§ 552a(a)(7), (b)(3).

²⁷ *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 548–49 (3d Cir. 1989).

²⁸ *Id.* at 549.

²⁹ *Id.* at 549–50 (citing *Mazaleski v. Treusdell*, 562 F.2d 701, 713 n. 31 (D.C.Cir. 1977)) (other citation omitted).

³⁰ 2025 DHS SAVE SORN at 48954.

³¹ 2025 Revised SSA SORN at 50883.

³² 2025 DHS SAVE SORN at 48954.

³³ See Puckett, *supra* note 23.

³⁴ *Id.*

³⁵ *Id.*

the SSA, Section 1106 of the Social Security Act (42 U.S.C. § 1306) establishes that the SSA and its employees are prohibited from disclosing information it collects, unless specifically authorized under federal law and regulations promulgated by the agency, imposing felonies for violations.³⁶ Underscoring the confidentiality of the SSA data and the narrow uses for which the data is permitted to be used, the Social Security Board's very first regulation, promulgated in 1937, addressed the narrow circumstances under which the SSA may disclose the data it collects.³⁷ To this day, the use of SSA data for vetting the citizenship status of voters is incompatible with the purposes for which such records were collected—that is, to administer Social Security programs.

Allowing the SAVE system to access SSA data contradicts years of warnings by SSA itself that the records it holds do not provide reliable information on U.S. citizenship or immigration status.³⁸ Indeed, it is DHS that is responsible for maintaining current immigration and work authorization status for all noncitizens.³⁹ Many SSA records may be outdated because an individual's immigration status may change after they apply for their SSN, and there is no obligation for an individual to report to SSA a change in their immigration status unless they are receiving Social Security payments.⁴⁰ A 2006 audit by SSA's Office of Inspector General estimated that SSA's citizenship data inaccurately identified about 3.3 million U.S. citizens as non-citizens "because they had become U.S. citizens after obtaining their SSN" and "had not updated their records with SSA."⁴¹ Further, there are inaccuracies in SSA citizenship data for U.S.-born citizens because the agency did not consistently collect and maintain this information before 1981.⁴² Verifying the citizenship status of registered voters is simply not a compatible application of records collected to administer public benefits, and the unfitness of the SSA data for such a purpose clearly attests to as much.

Naturalized citizens are most at risk for having incorrect citizenship information in SSA data because their status would have changed, and recent developments under the Trump administration heightens the risk for such citizens. In March of this year, SSA quietly paused the Enumeration Beyond Entry Program (EBE),⁴³ in which SSA processed automatically the issuance of new Social Security cards for noncitizens granted work authorizations and newly naturalized U.S. citizens if the individual authorized the transfer of information from USCIS to SSA to do so.⁴⁴ The EBE's continued pause requires recently naturalized citizens to request SSA

³⁶ 42 U.S.C. § 1306(a)(1); see *California ex rel. Younger v. Weinberger*, 505 F.2d 767, 768 (9th Cir. 1974).

³⁷ Social Security History, Regulation No. 1, SSA, <https://perma.cc/V8FR-24WX>.

³⁸ SSA Off. of the Inspector Gen., Cong. Resp. Rep. No. A-08-06-26100, *Accuracy of the Social Security Administration's Numident File* 13 (Dec. 18, 2006), <https://perma.cc/5G2J-FF4V> ("Accuracy of SSA Numident File").

³⁹ *Policy for U.S. Citizenship*, SSA (Feb. 23, 2024), <https://perma.cc/PJL4-MVCP>.

⁴⁰ Letter from SSA Off. of Gen. Counsel to Fair Elections Ctr. 2 (July 13, 2023), <https://fairelectionscenter.org/wp-content/uploads/2025/07/SSA-Touhy-Decision-letter.July-13-2023-signed.pdf> ("Letter from SSA to FEC").

⁴¹ Accuracy of SSA Numident File at 13.

⁴² Letter from SSA to FEC at 2.

⁴³ Judd Legum, *EXCLUSIVE: Secret Policy Shift could Overwhelm Social Security Offices with Millions of People*, Popular Information (Mar. 20, 2025), <https://popular.info/p/exclusive-secret-policy-shift-could>.

⁴⁴ Amy L. Peck & Otieno B. Ombok, *SSA Pauses Automatic Issuance of SSNs for Certain Immigration Applicants*, Jackson Lewis (June 11, 2025), <https://www.globalimmigrationblog.com/2025/06/ssa-pauses-automatic-issuance-of-ssns-for-certain-immigration-applicants/>.

to process a name change and update their citizenship status through an in-person visit to an SSA field office.⁴⁵ The quiet policy change with no public notice meant that newly naturalized citizens who requested the automatic processing for a new social security card on their USCIS forms may wait for months for a new social security card under the false belief that a new social security card is being processed. As a result, the SSA database will have outdated Social Security numbers for newly naturalized citizens unaware that they must undertake an in-person appointment to obtain a new social security number. The “pause” appears to be ongoing⁴⁶ despite the SSA website continuing to claim that the EBE program is still in effect, which furthers confusion.⁴⁷ In addition to creating confusion, unnecessary obstacles by requiring in-person appointments, and administrative burdens for field SSA staff,⁴⁸ the pause of EBE unnecessarily delays SAVE correctly reflecting that a newly naturalized person is a citizen, potentially for several months. This threatens the ability of recently naturalized citizens to vote in upcoming elections.

Put simply: SSA should know better. The overhauled SAVE system’s use of the last four digits of the SSN to query the system creates novel and unremedied risks of false identity matches, further evincing the unsuitability of such data for citizenship verification. While DHS purports to “enhance” voter verification by allowing SAVE queries using the last four digits of the SSN⁴⁹ instead of the full SSN, the last four digits of an SSN are not a unique identifier. In fact, a 2009 report by the SSA’s Office of Inspector General found that “up to 40,000 numberholders possibly share SSNs that have the same last four digits.”⁵⁰ A misidentification is not a remote possibility—in FY 2008, SSA produced 1,200 multiple match responses, which meant that in those instances, name, date of birth, and the last four digits of the SSN matched multiple individuals in SSA’s records.⁵¹ SSA’s disclosures are creating a real risk of misidentifying or mismatching individuals between the voter file and the data accessed by SAVE, leading to inaccurate results and the wrongful removal or burdening of registered voters.⁵²

SSA cannot pass the buck to DHS to ensure accuracy of SAVE’s outputs. SAVE’s purported additional verification procedures provide little confidence of preventing erroneous results, further underscoring the incompatibility of using the source data accessed for citizenship verification. The updated SAVE fact sheet states that USCIS cannot or will not conduct

⁴⁵ Michael Sainato, *Millions of Legal Immigrants’ Lives Upended after Social Security Freeze*, Guardian (June 3, 2025), <https://www.theguardian.com/us-news/2025/jun/03/social-security-program-quietly-frozen-musk-immigrant-claims>.

⁴⁶ See *id.*; r/USCIS, *Are SSN cards no longer being sent to immigrants?*, Reddit (Oct. 31, 2025), https://www.reddit.com/r/USCIS/comments/1okww61/are_ssn_cards_no_longer_being_sent_to_immigrants/; r/USCIS, *Automatic processing of SSNs for H-4 EAD application?*, Reddit (Sept. 17, 2025), https://www.reddit.com/r/USCIS/comments/1njc2y9/automatic_processing_of_ssns_for_h4_ead/.

⁴⁷ SSA, *Enumeration Beyond Entry* (Feb. 10, 2025), <https://perma.cc/G649-QW8W>.

⁴⁸ Letter from Gerald E. Connolly, Ranking Member, H. Comm. on Oversight and Gov’t Reform, to Leland Dudek, Acting Comm’r for Soc. Sec. Admin., at 2–3 (Apr. 16, 2025), <https://perma.cc/4RYF-Q6E8>.

⁴⁹ Press Release, *USCIS Enhances Voter Verification Systems*, USCIS (Nov. 3, 2025), <https://perma.cc/E8MF-GZY5>.

⁵⁰ SSA Off. of the Inspector Gen., No. A-03-09-29115, Quick Response Evaluation - Accuracy of the Help America Vote Verification Program Responses 6 (June 2009), <https://perma.cc/Y8CW-CHRQ>.

⁵¹ *Id.*

⁵² See 2025 DHS SAVE PIA at 19–20.

“additional verification” for queries with only an SSN and will only conduct additional verification if a DHS numeric identifier is provided by the user agency or found in querying SSA data.⁵³ SAVE’s additional verification procedures involve additional levels of manual verification conducted by USCIS employees and are “important for ensuring an accurate and complete response.”⁵⁴ User agencies are required to escalate cases when prompted by SAVE or when requested by the applicant.⁵⁵ However, the track record of user agencies suggests otherwise. A 2017 report by the U.S. Government Accountability Office (GAO) reflects that, from approximately 2012 to 2016, “the majority of SAVE user agencies that received a SAVE response prompting them to institute additional verification did not complete the required additional steps to verify the benefit applicant’s immigration status.”⁵⁶ None of the states’ SAVE Memoranda of Agreement (MOAs) for voter registration or list maintenance purposes address the unreliability and incompleteness of SSA citizenship data or the risk of error when using it for voter citizenship checks.⁵⁷ And DHS itself recognizes the risk in its PIA that SAVE user agencies “may not go through all steps to ensure accuracy of information.”⁵⁸ Despite such concerns, SSA still forges ahead, irresponsibly and unlawfully providing the SAVE system access to SSA data on hundreds of millions of individuals.

The dramatic expansion of the SAVE system, with the aid of SSA, for the purpose of verifying voters’ citizenship status violates the Privacy Act and threatens real harm of voter disenfranchisement and wrongful prosecution. The newly created risks of erroneous results from the SAVE system require naturalized citizens to update their citizenship status with SSA through in-person appointments—despite there being no legal obligation for them to do so, if not for the risk of disenfranchisement. Misidentification or an inconclusive response for voters may create additional burdens for the citizen to prove their citizenship to their voting jurisdiction. In fact, Texas, a SAVE user, has asked over 170 counties to send notices⁵⁹ to thousands of voters who have been flagged by the new SAVE system as “potential” non-citizen registered voters.⁶⁰ Early reports indicate a high error rate, with numerous eligible voters being wrongfully identified as

⁵³ *Voter Registration and Voter List Maintenance Fact Sheet*, USCIS (Aug. 27, 2025), <https://perma.cc/7S3Z-R6BU>.

⁵⁴ U.S. Gov’t Accountability Off., Rep. No. GAO-17-204, *Immigration Status Verification for Benefits: Actions Needed to Improve Effectiveness and Oversight* at 4 (Mar. 23, 2017), <https://perma.cc/KBX6-86CM>.

⁵⁵ USCIS, *SAVE User Reference Guide* Ch. 9.2 (July 16, 2025), <https://perma.cc/DE8W-9US6>.

⁵⁶ U.S. Gov’t Accountability Off., Rep. No. GAO-17-204, *Immigration Status Verification for Benefits: Actions Needed to Improve Effectiveness and Oversight* at 17–18 (Mar. 2017), <https://perma.cc/KBX6-86CM>.

⁵⁷ See, e.g., USCIS, *Voter Verification Agency Sample MOA Draft* (June 9, 2025), <https://perma.cc/7X59-4DF4>; MOA between the DHS, USCIS, and the Va. St. Board of Elections (Mar. 20, 2014), <https://www.courtlistener.com/docket/69234255/26/3/virginia-coalition-for-immigrant-rights-v-beals/>; *Texas Secretary of State Communications Concerning Voters Searched in SAVE*, American Oversight (June 18, 2025), <https://americanoversight.org/featureddocument/texas-secretary-of-state-communications-concerning-voters-searched-in-save/>.

⁵⁸ 2025 DHS SAVE PIA at 19–20.

⁵⁹ *Notice to Registered Voter for Proof of Citizenship (USCIS Verification)*, Tex. Sec’y of St. (Oct. 2025), <https://perma.cc/Q5XA-CW3R>.

⁶⁰ Press Release, *Texas Completes Citizenship Verifications in the SAVE Database*, Tex. Sec’y of St. Jane Nelson (Oct. 20, 2025), <https://www.sos.state.tx.us/about/newsreleases/2025/102025.shtml>; *List of Potential Non-Citizens*, Tex. Sec’y of St. Jane Nelson, <https://perma.cc/E3PX-X37P>.

non-citizens and forced to re-prove their citizenship status to prevent cancellation of their voter registrations within 30 days.⁶¹ Louisiana claims to have removed nearly 400 voters from their voter rolls using the SAVE system,⁶² and an October 2025 report by the Virginia Department of Elections says that between September 1, 2024, and August 31, 2025, 1,644 Virginia voter registrations were cancelled as a result of SAVE citizenship checks.⁶³ Requiring documented proof of citizenship of registered voters impermissibly burdens the right to vote, wrongfully risks disenfranchisement, and further underscores the unfitness of SSA data now being channeled into the SAVE system for use in voter verification.

b. The Do Not Pay routine use raises additional concerns about the creation of a national data bank within the Treasury Department.

This administration’s expansion of interagency data collection through the Do Not Pay routine use raises similar concerns about the creation of an illegal national data bank. In March 2025, President Trump issued an executive order titled “Protecting America’s Bank Account Against Fraud, Waste, and Abuse.”⁶⁴ Nominally intended to strengthen fraud detection and prevention, among others, the executive order directs agencies to update relevant SORNs to include a routine use to disclose personal data to the Department of Treasury for the Do Not Pay Working System (DNP).⁶⁵ DNP is a program that allows the Treasury to access data across agencies⁶⁶ to prevent and detect improper payments from the Treasury.⁶⁷ Aligned with this directive, the Notice purports to establish Routine Use 50, which would allow SSA to disclose records “[t]o the U.S. Department of the Treasury, when disclosure of the information is relevant to review SSA’s payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state ... in a state-administered, federally funded program.”⁶⁸

Routine Use 50 raises more questions than it answers and risks contributing to the transformation of the Do Not Pay system into an illegal and unaccountable national data bank. This routine use does not specify what information from SSA is “relevant” for DNP, thus failing provide notice to the public of what sensitive personal information may be implicated in such disclosures. In purporting to establish the new routine use to share SSA data for Do Not Pay,

⁶¹ Natalia Contreras, *Texas counties look into ‘potential noncitizens’ on voter rolls. Here’s what they’re finding.*, Votebeat Texas (Oct. 31, 2025), <https://www.votebeat.org/texas/2025/10/31/county-election-officials-investigate-potential-noncitizens-flagged-save-database/>.

⁶² Colin Vedros, *La. Secretary of State finds 390 registered illegally to vote in the state*, KALB (Sept. 4, 2025), <https://www.kalb.com/2025/09/04/la-secretary-state-finds-390-registered-illegally-vote-state/>.

⁶³ Va. Dept. of Elections, *Annual List Maintenance Report: September 1, 2024 – August 31, 2025*, at 19, <https://www.elections.virginia.gov/media/formswarehouse/maintenance-reports/2025-Annual-List-Maintenance-Report.pdf>.

⁶⁴ Exec. Order No. 14249, 90 Fed. Reg. 14011, 14011 (March 25, 2025).

⁶⁵ *Id.* at 3(d).

⁶⁶ *Do Not Pay: What Can I Search?*, Bureau of the Fiscal Service (last updated July 14, 2025), <https://perma.cc/9Y8E-ABHE>.

⁶⁷ *Do Not Pay*, Bureau of the Fiscal Service (last updated July 29, 2025), <https://perma.cc/24S5-RL9P>.

⁶⁸ 2025 Revised SSA SORN at 50883.

SSA and the Trump administration are attempting to skirt the safeguards and public accountability established by Congress in the Privacy Act. Under the Privacy Act, agencies typically must enter into Computer Matching Agreements before personal data from one agency can be cross-referenced with personal data from another for the provision of federal benefits.⁶⁹ However, the Department of Treasury, the agency operating the Do Not Pay system, in consultation with the Office of Management and Budget, may waive the requirements for a Computer Matching Agreement.⁷⁰ With this routine use in place, there is a heightened risk that the Treasury Department will link the databases across the federal government to operate DNP, effectively creating a national data bank. When those databases are cross-referenced without any published Computer Matching Agreements, the public will have far less insight and opportunity to hold the involved agencies accountable to their privacy obligations. Another national bank without adequate oversight creates ample opportunities for misuse and abuse of sensitive personal information.

III. The Notice reveals numerous other violations of federal law left unaddressed by SSA.

Even beyond its dubious discussion of routine uses, SSA's Notice reveals multiple other violations of the Privacy Act, the Social Security Act, and SSA's own regulations.

a. SSA is disseminating records it knows to be unreliable to a system it should know is inadequately protected, violating the Privacy Act along the way.

SSA lacks any legal basis for disclosing sensitive records to DHS. The agency only invokes 8 U.S.C. § 1373(a) to justify disclosing "citizenship and immigration information" (information it has previously stated it does not maintain)⁷¹ to DHS.⁷² But importantly, that law does not purport to override other federal laws prohibiting the disclosure of federal records to DHS, including the Privacy Act.⁷³ SSA fails to establish that its broad sharing of Social Security information with DHS is either "relevant" or "necessary to accomplish" any valid, legal purpose under § 1303(a) or the Social Security Act.⁷⁴ The Privacy Act requires a system of records to be both "relevant" and "necessary,"⁷⁵ but SSA neglects to address either element. Of course, it is difficult to imagine that SSA could ever establish necessity and relevance for aiding DHS's haphazard and sweeping expansion of the SAVE system. DHS's revisions to the SAVE system link massive amounts of sensitive information from across federal, state, and local governments,

⁶⁹ 5 U.S.C. § 552a(o).

⁷⁰ 31 U.S.C. § 3354(b)(3)(B).

⁷¹ Letter from SSA to FEC at 2 (stating that, while SSA records "provide an indication of citizenship," it is not definitive information on citizenship, which is maintained by DHS itself).

⁷² 2025 Revised SSA SORN at 50880.

⁷³ 8 U.S.C. § 1373(a) ("*Notwithstanding any other provision of Federal, State, or local law, a Federal ... government entity may not prohibit, or in any way restrict, any government entity from sending to, or receiving from [DHS] information regarding the citizenship or immigration status, lawful or unlawful, of any individual.*") (emphasis added).

⁷⁴ 5 U.S.C. § 552a(e)(1).

⁷⁵ *Id.*

creating just the kind of “national data banks” that Congress has explicitly considered and rejected.⁷⁶

SSA has made no effort to ensure that the information the agency now disseminates⁷⁷ to DHS for use in SAVE is accurate, timely, or complete, despite the sensitive nature of both the information and DHS’s stated use for determining voter eligibility.⁷⁸ Not only has SSA admitted that its citizenship data is incomplete, unreliable, and not “definitive,” but it has repeatedly warned that its data should not be used for making citizenship determinations.⁷⁹ Despite this, the agencies have pressed on. Now SSA’s inaccurate and incomplete data is disseminated to non-federal users through the SAVE system, which DHS encourages users to employ in ways that will disenfranchise many of their fundamental right to vote. These are blatant violations of 5 U.S.C. § 552a(e)(6).

Despite knowing that DHS will pipe sensitive information from SSA to the illegally overhauled SAVE system, SSA unjustifiably continues to grant DHS access to records the agency acknowledges are “very sensitive.”⁸⁰ In doing so, the agency joins DHS in creating significant security risks that the agency should anticipate and that the Notice does not adequately address.⁸¹ SSNs alone are highly valuable pieces of information. Once limited to a single purpose, SSNs are now necessary for anyone wishing to acquire credit, get a new job, or apply for housing—and along the way have become extremely valuable targets for identity thieves. Identity theft affects an estimated 500,000 and 700,000 people every year.⁸² Many of these incidents are made possible through the capture of a person’s SSN. But the SSN is not a standalone piece of information: vast quantities of sensitive personal information are keyed to an individual’s SSN, including their tax information, credit information, employment and education records, and medical information. This makes SSNs extremely valuable to identity thieves and other bad actors. At the same time, DHS has enabled SAVE users to conduct bulk uploads, undertaken a concerted effort to expand SAVE’s allowable uses, and enabled many users to access the cases and information of other system users. These changes to the SAVE system have made it an even more compelling honeypot for malicious third parties. Not only is the information housed in the system far richer; the entry points are now more numerous.

Threats to the SSA information contained in the SAVE system are not limited to external actors, however. DHS has diminished the SAVE system’s security and further endangered the privacy of affected individuals by enabling bulk uploads and allowing many SAVE users to

⁷⁶ See Pub. L. 100-503, § 9 (Oct. 18, 1988). Section 9(1) states that “[n]othing in the amendments made by this Act shall be construed to authorize... the establishment or maintenance... of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies.”

⁷⁷ 5 U.S.C. § 552a(e)(6) (requiring DHS to “make reasonable efforts to assure that [records] are accurate, complete, timely, and relevant for agency purposes” before it disseminates records to non-federal entities, such as states.).

⁷⁸ 2025 DHS SAVE SORN at 48950–51.

⁷⁹ Letter from SSA to FEC at 2.

⁸⁰ 20 C.F.R. § 401(105)(b).

⁸¹ See 5 U.S.C. § 552a(e)(10) (requiring SSA to establish safeguards to ensure the security and confidentiality of records and protect against anticipated threats or hazards).

⁸² *Government Records & Privacy*, EPIC, <https://epic.org/issues/data-protection/government-records-privacy/>.

access the cases and information uploaded by other users.⁸³ As a result of these new capabilities, control over the Social Security information given to SAVE users is limited and easily lost altogether. Any SAVE user could take advantage of these features to seed their own surveillance systems across the U.S., which in turn pose further security hazards and risks to civil liberties. SSA's Notice fails to account for any of these risks.

Finally, SSA should be well aware that DHS has not taken adequate steps to mitigate the risks invited by its use of Social Security records and other changes to the SAVE system. DHS's own Notice for the overhauled SAVE system invokes NARA retention schedule N1-566-08-007, a schedule developed in 2008 that does not contemplate a centralized repository like the one DHS has created and that proposes retaining records for a period of ten years, leaving ample room for the system and the information within it to be compromised.⁸⁴ DHS's Notice fails to meet the Privacy Act's high standards⁸⁵ for establishing safeguards, and SSA's Notice does not attempt to fill the gaps and address the risks of DHS's lossy approach to security. This is particularly unsettling in light of the federal government's long and sordid record of data breaches, including at OPM,⁸⁶ DHS,⁸⁷ CBP,⁸⁸ ICE,⁸⁹ and SSA.⁹⁰ The Notice not only fails to account for these hazards but identifies no mechanisms to detect, prevent, and ensure accountability for illegitimate access to, breach of, or use of SAVE information.

Between the lack of legal authority for including Social Security information in the SAVE system, DHS's deficient security measures, and SSA's intimate awareness of the harms that can result from the compromise of Social Security data, SSA should know better than to

⁸³ 2025 DHS SAVE SORN at 48948 (“Additionally, user agencies with appropriate legal authority may now view, within SAVE, other user agencies' case data through a linking mechanism based on either benefit type granted (e.g., Medicare) or by state. This new account type will have reporting options to view case data.”).

⁸⁴ 2025 DHS SAVE SORN at 48954–55.

⁸⁵ 5 U.S.C. § 552a(e)(10).

⁸⁶ See Hon. Jason Chaffetz, et al., *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, U.S. House of Rep. Comm. Oversight & Gov't Reform (Sept. 7, 2016), <https://perma.cc/4J5W-SX3W>.

⁸⁷ See, e.g., Megan Roos, *Suspected Russian SolarWinds Hack Compromised Homeland Security Department*, Newsweek (Dec. 14, 2020), <https://www.newsweek.com/suspected-russian-solarwinds-hack-compromised-homeland-security-department-1554656>. For many more examples of data breaches at DHS and its subcomponents, see *Comments to Dep't of Homeland Security on Collection of Biometric Data from Aliens Upon Entry to and Departure From the United States*, EPIC at 9–11 (Dec. 21, 2020), <https://epic.org/documents/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states/>. In fact, a September 2025 report from the DHS Office of the Inspector General found that an DHS high-value asset system containing sensitive information had inadequate cybersecurity and significant, exploitable weaknesses. See DHS OIG, *Inadequate Cybersecurity Rendered DHS Headquarters High-Value System Vulnerable to Attack*, OIG-25–43 (Sept. 23, 2025), <https://perma.cc/E62W-M2RM>.

⁸⁸ See Joseph Cuffari, *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot*, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020), <https://perma.cc/2R6G-KKHL>.

⁸⁹ See, e.g., Luke Barr, *Names, Personal Information of 6,000 Noncitizens Posted on ICE Website 'Erroneously,' ICE Says*, ABC News (Dec. 1, 2022), <https://abcnews.go.com/Politics/names-personal-information-6000-noncitizens-posted-ice-website/story?id=94308375>.

⁹⁰ Brumfiel, *supra* note 23.

disclose its records to DHS. SSA's actions violate the Privacy Act, and both the Notice and the agency's novel data disclosures should be immediately rescinded.

b. SSA exceeds its authority and violates both the Social Security Act and its own regulations by disclosing records to DHS and SAVE users.

SSA also strays far beyond its organic powers by disclosing records to DHS. Under threat of criminal prosecution, Section 1106 of the Social Security Act prohibits SSA from disclosing “any file, record, report, or other paper, or any information” obtained by the agency without explicit approval by another regulation or federal law.⁹¹ Several other sections of that Act similarly prohibit disclosure of SSA records obtained by States and other users administering benefits.⁹² Just as 8 U.S.C. § 1373(a) does not supersede the Privacy Act, it cannot negate the Social Security Act's several prohibitions on disclosure. Because it lacks any other lawful basis for disclosure, SSA is violating its own mandate. The agency knows this. In its longstanding policy on disclosure and verification of SSNs without consent, the agency states that it does “not have the legal authority to disclose information about U.S. citizens to DHS.”⁹³

Nor does anything in the agency's own regulations permit it to disclose these records.⁹⁴ SSA ordinarily ensures a high degree of protection for the records it maintains, understanding that it is the custodian of “often very sensitive information” from a “much greater number of persons” who are not able to opt out.⁹⁵ Where, as here, the SSA is under no legal obligation to disclose the personal data in question, SSA regulations require it to ask whether a disclosure of information would result in a “clearly unwanted invasion of personal privacy,” considering the sensitivity of the information, the public interest in disclosure, the rights and expectations of affected individuals, and the existence of safeguards against unauthorized redisclosure or use of the information.⁹⁶ That standard is easily violated here. The agency is now providing its Master Files—files it acknowledges to contain uniquely sensitive information—to DHS for use in the overhauled SAVE system without articulating any public interest. Alarming, SSA knows that the records are not protected from threats⁹⁷ of unauthorized redisclosure or use and that the records may be used to violate the fundamental rights of affected individuals. Even under the agency's own rules, these disclosures cannot be justified.

IV. SSA's lack of Computer Matching Agreements applicable to disclosing data for citizenship and immigration verification violates the Privacy Act.

The Notice does not identify or solicit public comment on any Computer Matching Agreements between SSA and the relevant agencies that would authorize SSA to carry out the proposed routine use of disclosing citizenship and immigration information to DHS. Absent such

⁹¹ 42 U.S.C. § 1306(a)(1).

⁹² See, e.g., 42 U.S.C. § 405(c)(2)(C)(viii)(I).

⁹³ SSA, *Disclosure and Verification of Social Security Numbers (SSN) Without Consent*, Program Operations Manual System (POMS), GN 03325.002 (2023), <https://perma.cc/ZB69-JTDX>.

⁹⁴ See 20 C.F.R. §§ 401.100 *et seq.*

⁹⁵ 20 C.F.R. § 401.105(b).

⁹⁶ *Id.* § 401.140.

⁹⁷ See Section III.a, *supra*.

agreements, SSA’s linking of data to DHS’s new matching program violates the computer matching restrictions of the Privacy Act.⁹⁸

Under the Privacy Act, a Computer Matching Agreement is required when agencies match datasets to determine federal benefit eligibility.⁹⁹ Matching agreements must include detailed data elements and meet strict requirements designed to ensure public transparency and participation, congressional and agency oversight, and rigorous legal compliance.¹⁰⁰ Like SORNs, an agency must provide advance notice to the public and Congress and opportunity for public comment whenever it establishes or significantly changes a matching program.¹⁰¹

The information sharing agreement between SSA, DHS, and USCIS regarding citizenship does not constitute a valid Computer Matching Agreement. The information sharing agreement was not posted on the Federal Register for a notice and comment period despite going into effect on May 15, 2025.¹⁰² The information sharing agreement is not included on SSA’s list of Computer Matching Agreements, which usually include links to the agency’s active matching program and its corresponding Federal Register notices.¹⁰³ Further, the information sharing agreement was publicly disclosed through a FOIA request via its FOIA Reading Room and solely refers to itself as a “letter agreement,” which is atypical of SSA Computer Matching Agreements.¹⁰⁴

This Notice and the information sharing agreement between DHS, USCIS, and SSA indicate that there is a new bulk matching of state, SSA, and DHS records for federal benefits determinations, among other purposes. Specifically, the agreement states that SSA will support DHS “by matching data submitted through SAVE to SSA records in [its] Master Files of Social Security Number (SSN) Holders and SSN Applications.”¹⁰⁵ The input of information from SAVE that is then sent to SSA to “confirm or not confirm that the SSN, name, and date of birth match information in SSA records” and indicate citizenship or immigration status¹⁰⁶ undoubtedly constitutes a new or revised “matching program” under the Privacy Act.¹⁰⁷ By definition, a “matching program” includes any “computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of . . . establishing or verifying the eligibility of . . . beneficiaries of . . . cash or in-kind assistance or payments under [a] Federal benefit program [.]”¹⁰⁸ And DHS claims that, as of November 3, the overhauled SAVE system has already “allowed federal agencies to submit over 110 million queries to help verify eligibility for federally funded benefits.”¹⁰⁹ Yet SSA has not specified or otherwise disclosed any Computer Matching Agreements that relate to the overhauled SAVE system or use

⁹⁸ See 5 U.S.C. § 552a(o).

⁹⁹ *Id.*

¹⁰⁰ See *id.* §§ 552a(o)(1)–(2).

¹⁰¹ See *id.* §§ 552a(e)(12), (r). See also OMB Circular No. A-108, *supra* note 5, at 18–19.

¹⁰² DHS-SSA SAVE Agreement at 10, 12.

¹⁰³ See *Computer Matching Programs*, SSA, <https://perma.cc/YUT7-4QAL>.

¹⁰⁴ See *FOIA Reading Room*, SSA, <https://perma.cc/5HHA-H7VM> (selecting “Proactive Disclosures (Current Year) in the drop-down menu).

¹⁰⁵ DHS-SSA SAVE Agreement at 4.

¹⁰⁶ *Id.*

¹⁰⁷ See *id.*

¹⁰⁸ 5 U.S.C. § 552a(o).

¹⁰⁹ *USCIS Enhances Voter Verification Systems*, USCIS (Nov. 3, 2025), <https://perma.cc/8BDA-2ZVX>.

in citizenship or immigration status verification in its Notice. By failing to disclose the agreements, SSA has deprived the undersigned organizations and the public of critical information to which they are entitled by law, as well as the opportunity to provide public comment on this sweeping new inter-governmental data matching.

There is no applicable Computer Matching Agreement between SSA and DHS that reflect this new bulk matching activity from this or last year.¹¹⁰ The only publicly disclosed SSA Computer Matching Agreement with DHS is related to SSA accessing DHS data to identify noncitizens that leave voluntarily or have been removed “to determine suspension of payments, nonpayments of benefits, and/or recovery of overpayments[.]”¹¹¹ But this agreement does not address accessing the overhauled SAVE system from either agency for its expanded use in verifying citizenship or immigration status for public benefits.

Given the scale and sensitivity of the overhauled SAVE system, it is incumbent on SSA to disclose any and all relevant Computer Matching Agreements. If SSA has not completed an applicable Computer Matching Agreement with DHS or relevant agencies utilizing the overhauled SAVE system, the agency must immediately deactivate and unwind such data transfer mechanisms until it has completed, publicly noticed, and published a Matching Agreement in accordance with the Privacy Act and OMB Circular A-108.

V. Conclusion

For the above reasons, SSA should promptly withdraw its Notice, immediately suspend the disclosure of personal records to DHS for citizenship and immigration purposes, and take the steps necessary to ensure that DHS and downstream SAVE users delete all personal records and derived data they wrongfully obtained as a consequence of such disclosures to date. If you require any additional information about SSA’s Privacy Act and related statutory obligations, please contact John Davisson, EPIC Director of Litigation, at davisson@epic.org.

Respectfully submitted,

Electronic Privacy Information Center (EPIC)
Advocacy for Principled Action in Government
Arab American Institute Foundation (AAI)
Association of Public Data Users
Center for Democracy & Technology
CTData Collaborative
Demand Progress Education Fund
League of United Latin American Citizens (LULAC)
National Women’s Law Center
New America’s Open Technology Institute
Secure Elections Network
Surveillance Technology Oversight Project

¹¹⁰ See *2025 SSA Annual Matching Activity Report*, SSA (May 30, 2025), <https://perma.cc/K2CB-8E5C>.

¹¹¹ *Computer Matching Agreement Between the SSA and the DHS*, SSA Match #1010 (Apr. 4, 2024), <https://perma.cc/C2ZD-XB3L>.

Temple University Institute for Law, Innovation &
Technology (iLIT)
The Leadership Conference on Civil and Human Rights