December 1, 2025

Roman Jankowski
Chief Privacy Officer, Privacy Office
Department of Homeland Security
Washington, DC 20528-0655

Re: Notice of a modified system of records to the Systemic Alien Verification for Entitlements (SAVE) Program by the U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services

UnidosUS respectfully submits these comments in response to the Department of Homeland Security's proposed modifications to the Systemic Alien Verification for Entitlements (SAVE) program system of records notice (SORN) published on October 31, 2025.

For more than 55 years, UnidosUS has advanced economic opportunity for Latino families and ensured that America's promise is open to all who contribute to its strength. With nearly 300 community-based Affiliates in 37 states, Washington, D.C., and Puerto Rico, we serve and advocate for millions of Latinos, including U.S. citizens by birth, naturalized citizens, and lawful permanent residents whose personal information will be affected by the proposed SAVE program modifications.

Unidos's Affiliate network and the communities they serve are deeply and directly impacted by the modifications proposed by the new SORN. DHS published this modified SORN on October 31, 2025, belatedly—more than five months after initially announcing the SAVE program's "overhaul" and four months after deploying this transformed system.

This after-the-fact notice cannot cure DHS's ongoing Privacy Act violations. DHS announcements characterize the proposed changes as an entire system "overhaul," confirming that these modifications are fundamental policy changes requiring, at the very least, full notice-and-comment rulemaking under the Administrative Procedure Act (APA) or new authorizing legislation and reconciliation with conflicting statutes. For such a major change with complex effects across a range of legal requirements, the APA requires notice-and-comment rulemaking to allow impacted parties, including communities that our Affiliate network serves, to meaningfully participate in the development of federal policy directly affecting their fundamental rights and privacy interests.

Disregarding these legal obligations, since May 2025, DHS has operated an unlawful system that fundamentally transforms SAVE from a specifically designed and limited immigration status verification tool into an expansive national citizenship database that

would consolidate highly sensitive personal information collected by the federal government for a wide range of purposes across multiple federal and state agencies.

DHS undertook this radical transformation in excess of its statutory authority and regardless of numerous statutory conflicts, without adequate safeguards, without appropriate and required notice to Congress or the public, and without assessing the severe risks of error that are already disenfranchising eligible citizens, leading to harmful and erroneous criminal investigations and potential denial of benefits to otherwise eligible individuals.

The impact of the DHS "overhaul" on Latinos is particularly severe given the prevalence of mixed-status households in our community. For example, U.S. citizens, including minors, who shared personal information with government agencies for legitimate purposes such as Medicaid enrollment, had no reason to believe, and were never informed, that their participation could increase deportation risk for family members through an unlawful effort to combine federal data across the government. These families relied on longstanding federal privacy protections that DHS has now flagrantly and unlawfully seeks to trample.

These comments describe how this modified SORN fundamentally lacks adequate safeguards, notice, or legal authority. The proposed modifications violate multiple provisions of the Privacy Act of 1974 and threaten the First and Fourth amendment rights of millions of Americans while creating severe risks of error that could result in wrongful denial of benefits, voter disenfranchisement, and baseless criminal investigations. For these reasons, UnidosUS strongly opposes this proposal and urges DHS to immediately withdraw this SORN, cease all operations of its unlawfully altered SAVE system, and restore SAVE to its original, authorized scope.

Background: The Privacy Act's Core Protections Against National Data Banks and SAVE's Original Limited Scope as a Targeted Immigration Status Verification Tool

The Privacy Act Was Enacted to Prevent "1984-Style" Government Dossiers and Centralized Federal Information Systems

The Privacy Act of 1974 was specifically enacted by Congress "to provide for protection against possible abuses of governmental power to affect an individual's privacy and confidential information… [especially] as our society enmeshes itself ever more deeply into the Information Age." The Act emerged from concerns about government surveillance during the Watergate and Counterintelligence Program (COINTELPRO) scandals, when federal agencies secretly and illegally compiled dossiers on American citizens deemed "subversive" and used personal information for unauthorized purposes.

As the U.S. Senate Committee on Government Operations' 1976 Source Book on Privacy explains, the Privacy Act was designed to prevent "formal or *de facto* national data banks" or "centralized Federal information systems" that could consolidate sensitive personal data stored across separate agencies. The Act's legislative history also makes clear that Congress established "robust safeguards against such 'interagency computer data banks' to make it 'legally impossible for the Federal Government in the future to put together anything resembling a '1984' personal dossier on a citizen.'"

SAVE's Original Authorization Limits the System to Individualized Immigration Status Queries for Specific Benefit Determinations, Explicitly Excluding the possibility of data sharing involving U.S.-Born Citizens as well as Social Security Number Searches

The SAVE program was originally established as a limited verification service enabling benefit-granting agencies to confirm the immigration status of benefit applicants when required by specific federal statutes. As originally authorized, the SAVE program permits queries of DHS immigration records to verify whether an individual who presents an immigration document is eligible for a particular benefit. In other words, this system permits only a targeted, individualized verification function tied to specific benefit applications from identified applicants.

USCIS guidance on use of the SAVE database, updated as recently as September 2025, explicitly states that the SAVE program:

- "does not verify U.S. born citizens under any circumstances,"
- "does not access databases that contain U.S.-born citizen information," and
- "cannot verify an individual's naturalized or acquired citizenship status using a Social Security Number, driver's license number, U.S. passport number, Consular Report of Birth Abroad, or other non-DHS documentation"

These limitations were not mere administrative choices. Instead, they reflect the legal parameters embedded in SAVE's statutory authorization.

Moreover, while the SORN cites several specific laws it identifies as allegedly authorizing use of the SAVE program, including the Immigration and Nationality Act, Immigration Reform and Control Act (IRCA), and Personal Responsibility and Work Opportunity Reconciliation Act (PRWORA), all of these laws only narrowly permit verification of immigration status for benefit eligibility determinations when individuals apply for specific public benefit programs. They do not authorize creation of a comprehensive database of U.S.-born citizens' personal information, systematic querying of Social Security employment records for voter verification, or bulk screening of entire populations. On the

whole the statute permits only targeted immigration status verification when legally required for benefit determinations—not data collection or comparisons for mass surveillance or election administration purposes.

The Proposed SORN Would Transform the Purpose, Nature, and Function of the SAVE Program, Constituting a Fundamental Policy Change that Both Exceeds the Department's Statutory Authority and Requires APA Rulemaking

DHS proposes to abandon SAVE's carefully delineated statutory boundaries and transform it into something Congress never authorized: a comprehensive national citizenship verification system that pools sensitive personal data across multiple federal agencies and makes it accessible to over 1,200 state and local government entities. This wholesale redesign would represent a major policy change that exceeds DHS's authority under the Privacy Act and require notice-and-comment rulemaking under the APA.

The APA requires notice-and-comment rulemaking when agencies make substantive policy changes affecting regulated parties' rights and obligations. (5 U.S.C. § 553). Courts have consistently held that agencies must use APA notice-and-comment rulemaking when making substantive policy changes that alter legal rights and obligations. Agencies cannot avoid this requirement by mischaracterizing such changes as procedural or informal actions. A SORN is legally inadequate for policy changes of this magnitude and complexity, and any agency attempting the kind of changes contemplated by this SORN must be invalidated as arbitrary and capricious (5 U.S.C. § 706(2)(A)).

The modified SAVE system requires DHS to reconcile multiple conflicting authorities among federal regulations and statutes, including but not limited to:

- The Privacy Act's prohibition on "national data banks" and interagency data pooling without Computer Matching Agreements;
- The National Voter Registration Act's rejection of documentary citizenship requirements and emphasis on expanding voter registration;
- Privacy protections for medical information that DHS now proposes to incorporate into SAVE.

These conflicts cannot be resolved through the SORN process, which provides for extremely limited notice and comment and does not require agencies to engage in reasoned decision-making, consideration of alternatives, analysis of costs and benefits, or detailed explanation of statutory authority that APA rulemaking demands.

This SAVE "overhaul" represents exactly the type of major policy change requiring APA rulemaking because it:

- fundamentally alters how millions of Americans' personal information will be collected, used, and shared;
- creates new obligations for state and local agencies;
- affects fundamental rights including privacy, voting, and access to benefits; and
- requires reconciliation of conflicting statutory authorities.

Notice-and-comment rulemaking would allow impacted parties, including UnidosUS, its nearly 300 Affiliates, civil rights organizations, voting rights advocates, state election officials, privacy experts, and concerned citizens to meaningfully participate in policy development. By using a SORN to accomplish this transformation, DHS has deprived impacted groups of these procedural rights and lacks the information necessary for reasoned decision-making.

The Privacy Act authorizes agencies to establish systems of records to accomplish specific statutory purposes. It does not authorize agencies to fundamentally repurpose existing systems to create new governmental functions that lack statutory authorization or, of course, that conflict with statutory obligations.

The modified SORN effects a policy transformation of the SAVE program in at least five critical respects, each of which independently exceeds DHS's statutory authority:

1. **Interagency Data Pooling Creates an Unauthorized National Data Bank**

The SORN now authorizes direct linking to or pooling from:

- SSA's Master Files of Social Security Number Holders (covering over 300 million Americans)
- Department of State passport records
- State motor vehicle department driver's license databases
- Certain sensitive medical information, and
- Information on sponsors and household members connected to individuals

The Computer Matching and Privacy Protection Act of 1988, which provides certain procedural amendments to the Privacy Act, expressly prohibits agencies from establishing "national data bank[s] that combine[], merge[], or link[] information on individuals maintained in systems of records by other Federal agencies" or "direct linking of computerized systems of records maintained by Federal agencies." By consolidating data from the SSA, the State Department, state agencies, and others, DHS has created a system to accomplish precisely what Congress expressly prohibits by statute.

2. Voter Verification Functions Exceed DHS' Statutory Powers and Produces Immediate Harm

The new SORN would explicitly authorize use of SAVE for "voter verification," including "verification of registrants and registered voters in voter registration and voter list maintenance processes." This would effectuate an unprecedented federal involvement in state voter registration processes that lacks statutory authorization and conflicts with existing federal voting rights laws.

As a federal court recently held in *League of Women Voters Education Fund v. Trump*, federal voting rights laws "forbid[] any individual of the Executive Branch from unilaterally exercising the delegated power to regulate State voter registration programs." (at 57). Specifically, DHS has no statutory authority to establish federal voter verification systems or impose documentary proof of citizenship requirements related to voter registration or voter verification. As that decision reaffirms, "our Constitution assigns responsibility for election regulation to the States and to Congress," not to the executive branch and clearly not to DHS.

The National Voter Registration Act (NVRA) establishes the legal framework for federal voter registration. The NVRA's stated purpose under 52 U.S.C. § 20501(b)(1) is "to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office." The NVRA requires only that voter registration forms include a citizenship question with attestation under penalty of perjury.

The Help America Vote Act (HAVA) reinforces this framework. Under 52 U.S.C. § 21083(b)(4)(A)(i), HAVA specifies that "The mail voter registration form developed under section 6 of the National Voter Registration Act of 1993…shall include the following: (i) The question 'Are you a citizen of the United States of America?' and boxes for the applicant to check to indicate whether the applicant is or is not a citizen of the United States."

Neither statute authorizes nor contemplates cross-checking voter registration applications against federal immigration or citizenship databases. By attempting to facilitate such cross-checks, the proposal to modify the SAVE program effectively imposes a back-end documentary proof of citizenship requirement—a policy Congress expressly rejected when enacting the NVRA and HAVA.

As detailed in UnidosUS' comments to the Election Assistance Commission on Oct. 20, 2025, approximately 21.3 million eligible voters — roughly 1 in 10 adult citizens — lack readily available documentary proof of citizenship such as birth certificates, passports, or naturalization certificates. SAVE-based voter verification would function as a *de facto* documentary proof requirement: when states cross-check voter rolls against SAVE and

receive non-confirmations for individuals whose SSA records are outdated or incomplete, those U.S. citizens and eligible voters could face wrongful removal from voter rolls, unless (theoretically) they can produce sufficient documentary proof to correct the database errors. Yet the SORN does not outline a process for correction for eligible citizens removed from voter rolls. This systematic exclusion of eligible citizens who cannot quickly obtain documents is precisely what the NVRA was designed to prevent.

Alarmingly, states are already using the overhauled SAVE system to purge voter rolls based on unreliable SSA data. As documented in ongoing litigation, Louisiana, Virginia, and Texas have begun removing voters and opening criminal investigations based on SAVE queries that incorrectly identify naturalized citizens as non-citizens. With the 2026 midterm elections next year, eligible citizens face imminent harm from erroneous conclusions drawn from these data.

3. **The Proposed Expansion to Include U.S.-Born Citizens Exceeds SAVE's Statutory Authorization**

For the first time under the new SORN, SAVE will query records belonging to U.S. citizens by birth. The laws cited as authority for SAVE, including the Immigration and Nationality Act, Immigration Reform and Control Act, and Personal Responsibility and Work Opportunity Reconciliation Act, authorize verification of immigration status for benefit eligibility determinations. They do not authorize creation of a comprehensive database of U.S. citizens' personal information.

4. **Social Security Number Matching Repurposes Data Beyond Statutory Authority**

The proposed new search-by-SSN functionality, including for U.S. citizens, relies on SSA citizenship data that the SSA itself has warned is incomplete and unreliable. In the Touhy decision, the SSA has stated that its "records do not provide definitive information about an individual's citizenship status" because the data represents only "a snapshot of the individual's citizenship status at the time of their interaction with SSA."

The Social Security Act authorizes SSA to collect information for Social Security benefit administration, not to create a national citizenship database accessible to immigration and election officials. Neither the Privacy Act nor any other statute authorizes DHS to repurpose SSA employment and benefits records for immigration enforcement or voter verification.

5. **The Proposal to Use Bulk Query Processing Fundamentally Alters SAVE's Operational Scope and Function**

The "list processor" feature proposed in the new SORN allows other agencies to upload files containing potentially millions of records for simultaneous processing, eliminating individualized review and dramatically increasing the risk of mass errors affecting eligible citizens. The statutory authorities and guidance materials cited above and throughout the modified SORN contemplate verification only when an individual applies for a specific benefit, not dragnet queries of entire populations.

These transformative changes have been undertaken without proper legal authority, adequate safeguards, or analysis for statutory compliance. A federal agency cannot exploit the SORN process to accomplish what would otherwise require congressional legislation and APA notice-and-comment rulemaking. Harms associated with this programmatic overhaul are not theoretical. Eligible citizens are already being wrongfully removed from voter rolls, denied benefits, and subjected to criminal investigation based on this unlawfully expanded system.

The Modified SORN Violates Multiple Privacy Act Requirements Designed to Ensure Transparency, Accuracy, and Accountability and Protect Americans from Governmental Overreach.

In addition to exceeding its statutory authority, DHS has also violated the Privacy Act's mandatory procedural and substantive requirements. The Act imposes mandatory requirements for any agency "system of records," defined as any group of records controlled by an agency from which information is retrieved by the name or some unique identifier of an individual. (5 U.S.C. § 552a(a)(5)). The proposed SAVE modifications violate these requirements— both wholesale in terms of the statutory scheme and in at least eight specific ways.

1. **DHS Has been unlawfully deploying a modified SAVE database**

DHS published this SORN on October 31, 2025, more than five months after it announced the overhaul of SAVE on April 22, 2025, and four months after it deployed the transformed system on May 22, 2025. Such after-the-fact notice cannot cure DHS' ongoing violation of the Privacy Act or its obligations under the APA, which require agencies to publish notice and solicit public comment before establishing or significantly changing systems of records. 5 U.S.C. §§ 552a(e)(4), (11).

For these reasons, since May 2025, DHS has been operating an unlawful system in direct violation of mandatory statutory safeguards. The Privacy Act's notice requirements exist precisely to prevent agencies from completing transformations of sensitive data systems in ways that are counter to law or that the public cannot meaningfully influence. By 'overhauling' SAVE first and publishing this SORN months later, DHS is depriving the public,

Congress, and affected individuals of their statutory rights to review and comment on proposed changes before implementation. This procedural violation alone requires withdrawal of this SORN and immediate cessation of the unlawfully transformed SAVE system's operations.

2. **Routine Uses L and M Violate Compatibility Requirements by Authorizing Wholesale Repurposing of Data Collected Under Entirely Different Statutory Authorities for Fundamentally Incompatible Purposes**

The Privacy Act prohibits agencies from disclosing any record contained in a system of records without express prior consent from an affected individual. This prohibition is subject to twelve limited exceptions, including the "Routine Uses" exception, which permits agencies to disclose information only for purposes that are "compatible with the purpose for which [the information] was collected." (5 U.S.C. § 552a(b)(3)).

The proposed modifications violate this requirement in three fundamental ways. First, the proposed SORN authorizes using SAVE for voter verification and voter list maintenance. This is an attempt to thoroughly repurpose data collected under entirely different statutory authorities for fundamentally incompatible purposes. For example, the SSA collects employment authorization data under the Social Security Act for benefits administration, not election oversight. The State Department issues passport documents under its foreign affairs authority for international travel, not for domestic voter verification. State motor vehicle departments collect driver's license information under state traffic safety laws, not federal citizenship verification statutes. Using employment records to verify voter eligibility, travel documents to purge voter rolls, and traffic safety data for election administration have never before been understood as "compatible" purposes and instead represent an effort to repurpose data in the precise way that the Privacy Act was designed to prevent.

Second, proposed Routine Use L authorizes sharing with "other federal, state, tribal, territorial, local governments and other authorized entities to assist user agencies determine U.S. citizenship." This language is impermissibly expansive and provides no meaningful limitation whatsoever. The phrase "assist user agencies determine" could encompass virtually any information sharing tangentially related to citizenship questions. The inclusion of "other authorized entities," for example, creates unlimited disclosure authority to undefined recipients for undefined purposes. DHS cannot bootstrap statutory authority it lacks by simply declaring that data collected for one statutory purpose can magically become "compatible" with entirely different governmental functions that Congress never authorized.

Third, proposed Routine Use M authorizes sharing for undefined "oversight" and "auditing" with unspecified "federal, state, territorial, tribal, local, and other entities." These terms are also overly broad and could encompass any activity, from routine program evaluation to criminal investigations. By mischaracterizing systematic interagency data pooling as "auditing," DHS is attempting to circumvent the Privacy Act's computer matching provisions, which require, *inter alia*, specific written agreements, Data Integrity Board review, cost-benefit analysis, and public disclosure.

3. **The SORN Fails to Provide Required Specificity About Which Agencies May Access Records, for What Purposes, and Under What Safeguards**

The Privacy Act clearly requires agencies to publish detailed SORNs in the Federal Register describing what records are maintained, how they are used, and with whom they are shared. Specifically, SORNs must include "each routine use of the records contained in the system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D)). Routine use descriptions must be "sufficiently specific to allow an individual to make an informed judgment about whether to provide personal information to an agency."

The SORN violates this requirement by failing to specify:

- Which specific agencies or entities may receive records under Routine Uses L and M;
- What specific determinations agencies will make or the actions that agencies may take;
- How long agencies may retain information or any other safeguards that protect against misuse;
- What specific data elements from SSA, State Department, and state motor vehicle sources will be maintained;
- How frequently data will be updated or what happens when source data conflicts.

In short, individuals reading these routine uses cannot ascertain whether their information might be shared with state election officials, local law enforcement, or federal prosecutors — or for what specific purpose.

4. **DHS is Repurposing Decades-Old SSA, State Department, and Motor Vehicle Records Without Providing Required Notice to More than 300 Million Affected Americans.**

The Privacy Act requires that when collecting information directly from individuals, agencies must (at the time of collection) inform them of the authority, purpose, and routine uses for information collected, and describe the consequences of not providing the requested information. 5 U.S.C. § 552a(e)(3). This requirement enables individuals to make informed decisions about providing personal information to the government and to protect their privacy interests.

The SORN violates this requirement by repurposing existing data without required notice:

- More than 300 million Americans whose SSA records SAVE will now query received no notice when applying for SSNs that their information would be used for voter verification, immigration enforcement, or disclosure to 1,200+ agencies;
- Passport applicants received no advance notice their international travel documents would be used for domestic voter list maintenance;
- State driver's license applicants received no prior notice DHS would access their information for citizenship verification;
- Voters whose registration lists are uploaded in bulk receive no advance notice that their information will be submitted to a federal immigration database.

In sum, the SORN provides no mechanism for notifying individuals whose decades-old records are being repurposed or when their information is accessed, queried, or shared.

5. **The SORN Incorporates Data Not Relevant or Necessary for Immigration Status Verification, and Authorizes Speculative Bulk Queries Without Individualized Justification Contrary to Law**

The Privacy Act requires agencies to maintain only information that is "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."(5 U.S.C. § 552a(e)(1). This core data minimization principle prevents agencies from building comprehensive dossiers 'just in case' information might prove useful at a later time. The proposed modifications violate this requirement in three ways.

First, the SORN incorporates data that is not relevant or necessary for immigration status verification, including, at least:

- Children's medical records and biometric identifiers from HHS,
- tax information,
- employment histories, and

- Excessive details regarding sponsors and household members (including phone numbers, marriage dates, and naturalization locations).

Second, the proposed bulk query feature violates the individualized necessity requirement. Uploading entire voter registration lists or benefits databases constitutes speculative querying without any showing of a particularized need. In doing so, the SORN seeks to permit indiscriminate data collection that the statute's 'relevant and necessary' requirements clearly prohibit.

Third, retaining state voter registration data submitted through bulk uploads is neither relevant nor necessary to achieve the SAVE program's statutorily authorized benefits verification purpose and is therefore contrary to law.

6. The Modified System Relies on SSA Citizenship Data That SSA Itself Warns Is Incomplete, Unreliable, and Not Definitive, Violating Statutory Accuracy Requirements

The Privacy Act requires agencies to maintain records that are "accurate, relevant, timely, and complete" to ensure fairness in determinations involving an individual. 5 U.S.C. § 552a(e)(5). Specifically, agencies must maintain records used in making determinations about individuals "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."

Citizenship data collected by the SSA and contained in its SSN Master Files—especially for naturalized citizens and U.S.-born citizens born before 1981—is incomplete, unreliable, and not definitive. There are three key limitations to the SSA's citizenship data that fail to meet the Privacy Act's accuracy requirements:

- The SSA's citizenship data is incomplete, even for native-born citizens. For SSNs issued before 1972, SSA did not require evidence of citizenship, and SSA did not consistently collect citizenship information until 1981. In these cases, SSA requires citizenship verification only when a person applies for benefits or requests a replacement Social Security card. Even now, many U.S. citizens who are born abroad, such as children of military personnel, do not have accurate citizenship data in SSA's SSN Master Files.

- The SSA's citizenship data is out of date, particularly for naturalized citizens. For most of the SSA's history, its records only reflect an individual's naturalized citizenship once they visited a local office with their documents. This created significant lags, since there was no requirement for SSN-holders to update their status with SSA until they got a replacement card or claimed benefits.

- The only citizenship data SSA possesses is provided by the individual at a single moment in time—i.e., when someone applies for an SSN and the corresponding card, or when they apply for benefits. SSA has no process for automatically updating the citizenship data it maintains, but rather relies on SSN-holders to inform SSA of any change in their status.

7. DHS Failed to Execute or Disclose Required Computer Matching Agreements with SSA, State Department, or State Motor Vehicle Departments, Circumventing Mandatory Data Integrity Board Review and Public Transparency

The Privacy Act requires that when agencies engage in automated comparison of records across systems, they must execute written matching agreements with specific safeguards and obtain Data Integrity Board review. (5 U.S.C. § 552a(o)). These agreements must include cost-benefit analysis demonstrating the program is "likely to be cost effective."

The SORN violates this requirement by:

- Failing to execute (or disclose execution of) matching agreements between DHS and SSA, State Department, or state motor vehicle departments;
- Providing no indication that there was a Data Integrity Board review assessing the proposal's accuracy, completeness, or cost-effectiveness; and
- Omitting a cost-benefit analysis that demonstrates that the program is "likely to be cost effective."

8. The SORN Fails to Establish Adequate Administrative, Technical, and Physical Safeguards Commensurate with Consolidating Sensitive Data from Multiple Agencies

The Privacy Act requires agencies to establish "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records" and prevent "substantial harm, embarrassment, inconvenience, or unfairness." (5 U.S.C. § 552a(e)(10)). Additionally, agencies must establish rules of conduct and provide training for persons involved in the system's operation. (5 U.S.C. § 552a(e)(9)).

The proposed SORN violates this requirement by:

- Failing to establish security standards commensurate with consolidating sensitive data from multiple agencies into a system accessible by 1,200+ user agencies;
- Establishing no audit mechanisms, accountability structures, or performance metrics for accuracy, error correction, or redress for decisions; and

- Creating bulk data exposure risks through the list processor feature in the absence of adequate data security safeguards.

Such violations are not mere technical deficiencies. Rather, they represent systematic noncompliance with the Privacy Act's core protections. DHS cannot lawfully implement its proposal without first complying with the mandatory safeguards Congress enacted to protect Americans' privacy.

DHS Must Immediately Withdraw This SORN, Cease All Unlawful Operations, and Restore SAVE to Its Original Authorized Scope to Prevent Further Irreparable Harm to Voting Rights and Privacy

UnidosUS strongly opposes this modified SORN and urges DHS to immediately withdraw it, cease all operations of the unlawfully transformed SAVE system, and restore SAVE to its original authorized scope as defined in the May 27, 2020 SORN. DHS has operated this system in violation of the Privacy Act and Administrative Procedures Act for five months, and now is attempting to use a SORN to accomplish what would require both Congressional authorization and APA notice-and-comment rulemaking.

Indeed, a federal court recently confirmed that unlawful government data sharing violates the common-law tort of breach of confidence, causing concrete injury independent of downstream harms. In *Center for Taxpayer Rights v. Internal Revenue Service*, the D.C. District Court held that Section 6103 of the Internal Revenue Code "establishes a relationship of trust between taxpayers and the IRS because it creates the general rule that the IRS must keep taxpayer information confidential." The court explains that when an agency breaches this duty by unlawfully sharing information, "the harm…occurs when the plaintiff's trust in the breaching party is violated, whether or not the breach has other consequences."

The same analysis applies with equal force here. The Privacy Act, the statutes authorizing specific public benefit programs and data collection, and SAVE's original limited scope establish a relationship of trust between SSN holders, passport holders, benefit applicants, and the federal government. Millions of U.S. citizens, naturalized citizens, and lawful permanent residents provide sensitive personal information to federal agencies and state motor vehicle departments based on explicit, and often even statutory, assurances that this data would be protected and used only for authorized purposes. DHS's transformation of SAVE into a comprehensive national citizenship database accessible to over 1,200 entities breaches this fundamental trust and causes concrete harm even before the system produces its inevitable rights violations and errors.

Nevertheless, harms associated with this programmatic overhaul are not theoretical. American citizens across the country could be wrongfully purged from voter rolls, denied benefits they may otherwise be eligible for, and subjected to baseless criminal investigations based on incomplete and unreliable data. Given these illegalities, DHS must act immediately to prevent further irreparable harm to the privacy, voting rights, rights to public benefits, and dignity of the millions of families nationwide.