

December 1, 2025

*Submitted via Federal e-Rulemaking Portal*

Roman Jankowski  
Chief Privacy Officer  
Privacy Office  
Department of Homeland Security  
Washington, D.C. 20528-0655

RE: Comment in Opposition to Modifications to and Reissuance of “DHS/USCIS-004 Systematic Alien Verification for Entitlements Program System of Records” (USCIS-2025-0337)

Dear Mr. Jankowski:

The undersigned Secretaries of State of California, Connecticut, Massachusetts, Maine, Michigan, Minnesota, New Jersey, New Mexico, Oregon, Rhode Island, Vermont and Washington submit the following comments in response to the Department of Homeland Security’s (DHS) proposal to modify and reissue the DHS system of records notice (SORN) titled “Department of Homeland Security/U.S. Citizenship and Immigration Services (USCIS)-004 Systematic Alien Verification for Entitlements Program (SAVE),” as noticed on October 31, 2025, in the Federal Register.<sup>1</sup> Put simply, we oppose DHS’s current approach to the expansion of SAVE for voter eligibility determinations, as reflected in the SAVE SORN.

While DHS claims that its changes to SAVE make it an effective tool for voter eligibility verification, the modifications to SAVE<sup>2</sup> are likely to degrade, not enhance, State efforts to ensure free, fair, and secure elections.<sup>3</sup> The expanded version of SAVE will introduce unnecessary and unwarranted reliability, privacy, and security issues into the sensitive voter information data we are entrusted to protect. It is likely to misidentify eligible voters as non-citizens and to chill participation by eligible voters. It has not been proven an accurate or reliable source of data for voter verification purposes, and there is significant cause for concern on this score.

---

<sup>1</sup> See Dep’t of Homeland Sec., *Privacy Act of 1974: System of Records*, 90 Fed. Reg. 48948, 48948-48955 (2025) (“DHS SORN”), <https://www.govinfo.gov/content/pkg/FR-2025-10-31/pdf/2025-19735.pdf>.

<sup>2</sup> For clarity, when we refer to “SAVE” throughout this comment, we are referring to the modified system as noticed by DHS in the Federal Register on October 31, 2025, unless the context makes clear, as here, that we are discussing modifications to the preexisting program. Where we seek to refer to the preexisting program, we will do so expressly by referencing SAVE’s earlier version.

<sup>3</sup> Indeed, some of the undersigned Secretaries are expressly barred from using SAVE under state law.

What the modified system will do, however, is allow the federal government to capture sensitive data on hundreds of millions of voters nationwide and distribute that information as it sees fit. It will facilitate the federal administration's attempt to claim for itself states' authority to regulate and administer elections. And it threatens to expose hundreds of millions of Americans' private data to cyberattack and misuse.

And all these risks must be considered against a single backdrop: American elections are free, fair, and secure. Study after study confirms that the so-called "problem" that SAVE targets does not exist: Non-citizen voting is exceedingly rare. As a result, although the undersigned Secretaries welcome appropriate, reliable, and secure tools to support our list-maintenance efforts, using SAVE as the administration intends presents unacceptable risks to our eligible voters. For all these reasons, and as further explained below, we oppose DHS's current approach to SAVE expansion and the resulting SAVE SORN.

## **I. Introduction and Summary**

As the Chief Election Officers for our States, the undersigned Secretaries have significant concerns related to the modifications to the DHS SORN and changes to SAVE, especially as those changes bear on voter-eligibility verification. The SORN fails to resolve existing concerns with earlier versions of SAVE to verify voter eligibility—and it prompts significant, new concerns. The dramatic increase in the number of people whose data could be ingested into SAVE amplifies these concerns. Instead of a program that has been used to verify the immigration and citizenship status of individuals applying for or receiving public benefits, SAVE now has the potential to encompass registered voters nationwide—that is, over 210 million people representing over 85% of the citizen voting age population.<sup>4</sup>

In expanding SAVE, DHS has moved from a system that queried its own records based on individual submissions to verify a single foreign-born registrant's citizenship status using limited immigration identifiers, to one that allows for bulk investigation of the citizenship of all registrants, including U.S.-born citizens, based on data from disparate agency databases and sources.<sup>5</sup> SAVE ingests state-held data and uses sensitive personal identifiers like a voter's full or partial Social Security number (SSN) to query information held by federal, state, and even private entities for further information related to the individual.<sup>6</sup> Queries could be directed to return information bearing on a voter's U.S. citizenship by searching records held

---

<sup>4</sup> Press Release, United States Election Assistance Commission, *U.S. Election Assistance Commission Releases 2024 Election Administration and Voting Survey (EAVS) Report* (June 30, 2025), <https://www.eac.gov/news/2025/06/30/us-election-assistance-commission-releases-2024-election-administration-and-voting>.

<sup>5</sup> DHS SORN at 48950-49851.

<sup>6</sup> DHS SORN at 48950-48951 (reflecting DHS's intent for SAVE to rely on the National Law Enforcement Telecommunications System ("NLETS")). *See id.* at 48953; *see also* Part V, *infra*.

by the Social Security Administration and thousands of law enforcement agencies, for example, as well to gather further identifiers—for example, driver’s license number and full SSN<sup>7</sup>—where that information is not provided by the voter or registered user.<sup>8</sup> SAVE then amasses this information into enhanced records that are retained for the next decade.<sup>9</sup> And these enhanced, retained records could be disclosed to a wide array of federal, state, local, and even private agencies and organizations.<sup>10</sup>

The changes to the SAVE program are likely to produce unreliable results and subject eligible voters to unnecessary burdens, intrusive investigations, and even disenfranchisement. They will allow DHS to amass and retain sensitive personal information on over a hundred million registered voters from disparate data sources and to use that data in a myriad of ways. And these dramatic changes have been proposed after only a short few months of development, with minimal testing that was conducted with no transparency or any meaningful explanation as to how this sensitive private data would be protected against security vulnerabilities and misuse.<sup>11</sup> In view of these shortcomings, the undersigned Secretaries must oppose DHS’s rollout of expansions to SAVE and the SAVE SORN. SAVE will not support our efforts to ensure the security of our citizens’ private data and promote free, fair, and secure elections.

The undersigned Secretaries and our States have long histories of conducting secure and accurate elections consistent with state and federal law. We faithfully discharge our responsibilities, including those under the federal National Voter

---

<sup>7</sup> DHS SORN at 48951 (describing how SAVE will “gain access” to further identifiers by accessing state driver’s license systems and NLETS).

<sup>8</sup> DHS SORN at 48950-48951 (describing changes to “*Enumerators and Source Systems*” that reflect access to SSA records, State Department records, state driver’s licensing agencies, and “national agencies that store driver’s license information for legal purposes (such as the National Law Enforcement Telecommunications System (NLETS))”).

<sup>9</sup> DHS SORN at 48951 (stating DHS anticipates using driver’s license numbers to “gain access to other government enumerators” that, in turn, “allow SAVE to match against other sources to verify immigration status and U.S. citizenship”); *id.* at 48950-48952 (stating that SAVE’s response becomes part of an individual’s case record in SAVE); *id.* at 48954-48955 (ten-year retention requirement).

<sup>10</sup> DHS SORN at 48954 (“Routine Uses”); *see also id.* at 48951 (describing the wide scope of records available to “user agencies with a legal authority to monitor and audit benefits granted or voter registration records” or “user agencies with appropriate legal authority”) (emphasis added); *id.* at 48954 (reiterating this routine use in paragraph “M” for entities with oversight authority).

<sup>11</sup> *See* News Releases, USCIS, *USCIS Deploys Common Sense Tools to Verify Voters* (May 22, 2025), <https://www.uscis.gov/newsroom/news-releases/uscis-deploys-common-sense-tools-to-verify-voters>; USCIS, News & Alerts, *Optimizing SAVE: New Options to Create Cases with a Social Security Number and by Bulk Upload* (May 22, 2025), <https://www.uscis.gov/save/current-user-agencies/news-alerts/optimizing-save-new-options-to-create-cases-with-a-social-security-number-and-by-bulk-upload>; USCIS, News & Alerts, *SAVE Optimization: SAVE Enhances the Bulk Upload Process* (Jul. 21, 2025), <https://www.uscis.gov/save/current-user-agencies/news-alerts/save-optimization-save-enhances-the-bulk-upload-process>; USCIS, News & Alerts, *Updated Guide to Understanding SAVE Verification Responses* (Jul. 30, 2025), <https://www.uscis.gov/save/current-user-agencies/news-alerts/updated-guide-to-understanding-save-verification-responses>.

Registration Act of 1993 (the “NVRA”)<sup>12</sup> and the Help America Vote Act of 2002 (“HAVA”)<sup>13</sup> to ensure current and accurate voter lists. So that elections are run in the manner best suited to each State’s unique populations, the U.S. Constitution and federal law reserve these duties to the States and, in turn, to our offices.

We embrace these duties and rely on proven tools to ensure the reliability of the information our offices possess, including as to voter eligibility. We both welcome and require reliable, properly secured data for these purposes. But the DHS SORN reveals reasons to doubt both the reliability and the security of the data SAVE retains and provides. If anything, by using SAVE in its modified form we risk inviting errors and discrepancies into the data we are entrusted to manage. And our use of a fundamentally flawed system to search for rare or non-existent instances of registered non-citizens would place a highly disproportionate burden on all eligible voters in our States—as to both their voting rights and privacy interests.

Indeed, the undersigned Secretaries have significant concerns that SAVE harms, rather than helps, the electoral process. SAVE risks misidentifying eligible voters as non-citizens. This likely is particularly so for older Americans, naturalized citizens, and voters like married women who have changed their names. Yet the flaws in the system likely may reach further than we can predict, unnecessarily creating problems for significant numbers of eligible voters. In practice, any SAVE response calling a voter registrant’s U.S. citizenship into question will require our offices to expend substantial time and energy to ensure that eligible, properly registered voters are not wrongly identified as non-citizens. As election-related budgets are already stretched thin, that time would necessarily come at a cost to our offices’ attention to other, vital duties—including *reliable* list maintenance procedures.

To be sure, only U.S. citizens may vote in federal elections. Our offices are assured of voter eligibility through the attestation procedures and associated penalties that Congress established for individuals who seek to register to vote in federal elections and, when appropriate, through tried-and-true methods that do not carry the same risks as SAVE. States already have laws on the books to ensure the security and accuracy of voter rolls. And there is no evidence that non-citizen registration or voting is even a problem, much less one in search of such a costly solution. State-level audits and reviews have shown that only a vanishingly small number of individuals are even *suspected* non-citizen voters, comprising only a

---

<sup>12</sup> See 52 U.S.C. §§ 20501-20511. The requirements of the NVRA apply to 44 States and the District of Columbia. Six States—Idaho, Minnesota, New Hampshire, North Dakota, Wisconsin, and Wyoming—are exempt from the NVRA because, on and after August 1, 1994, they either had no voter-registration requirements, or had election-day voter registration at polling places, with respect to elections for federal office. See 52 U.S.C. § 20503(b).

<sup>13</sup> See 52 U.S.C. §§ 21081-21085.

fraction of a percentage of votes cast in recent elections.<sup>14</sup> And other studies regularly reveal similar findings.<sup>15</sup> The modifications to SAVE attempt to solve a problem that doesn't exist at the expense of mistakes that could cost our citizens their most fundamental rights.

The modifications to SAVE also significantly intrude on our voters' privacy and virtually ensure continued intrusions. SAVE gathers sensitive, individualized information from registered users, including state agencies, and searches data held

---

<sup>14</sup> For example:

- The Michigan Department of State recently conducted a review that identified only 15 credible cases of possible noncitizen voting out of more than 5.7 million ballots case. That is an incidence rate of only 0.00028%. See Press Release, Mich. Dep't of State, *Michigan Department of State review confirms instances of noncitizen voting are extremely rare* (Apr. 3, 2025), <https://www.michigan.gov/sos/resources/news/2025/04/03/michigan-department-of-state-review-confirms-instances-of-noncitizen-voting-are-extremely-rare>.
- The North Carolina State Board of Elections identified just 41 individuals who were non-citizens with lawful immigration status (e.g., a green card) who cast a ballot out of the state's 4.8 million voters in the 2016 Presidential Election. N.C. State Bd. of Elections, *Post-Election Audit Report* at 2 (Apr. 21, 2017), [https://s3.amazonaws.com/dl.ncsbe.gov/sboe/Post-Election%20Audit%20Report\\_2016%20General%20Election/Post-Election\\_Audit\\_Report.pdf](https://s3.amazonaws.com/dl.ncsbe.gov/sboe/Post-Election%20Audit%20Report_2016%20General%20Election/Post-Election_Audit_Report.pdf).
- In 2011, the Colorado Secretary of State found 141 non-citizens on the state voter roll, representing .004 percent of the state's nearly 3.5 million voters. Mary Winter, *Covering the search for noncitizen voters*, Columbia Journalism Review (Oct. 22, 2012), [https://www.cjr.org/united\\_states\\_project/covering\\_the\\_search\\_for\\_noncitizen\\_voters.php](https://www.cjr.org/united_states_project/covering_the_search_for_noncitizen_voters.php). Ultimately, after a months-long effort, only 35 non-citizens who cast votes in past elections were identified.

<sup>15</sup> For example:

- The Heritage Foundation maintains a database with a “sampling” of election fraud cases prosecuted across the country—a Washington Post review of this database found only 85 cases involving alleged non-citizen voting over 20 years (i.e., 2003 to 2023). See Glenn Kessler, *The truth about noncitizen voting in federal elections*, Wash. Post (Mar. 6, 2024), <https://www.washingtonpost.com/politics/2024/03/06/truth-about-noncitizen-voting-federal-elections/>. In that 20-year period, more than one billion votes were cast in federal elections. *Id.* Eighty-five prosecutions represents an infinitesimal (0.000007%) amount.
- A study of 42 jurisdictions with high non-citizen populations found only 30 cases of suspected non-citizen voting in the 2016 Presidential Election across jurisdictions representing 23.5 million votes—an incidence rate of 0.0001 percent. Douglas Keith et al., *Noncitizen Voting: The Missing Millions* at 1, Brennan Center (May 5, 2017), <https://www.brennancenter.org/our-work/research-reports/noncitizen-voting-missing-millions>.
- An earlier Department of Justice's Ballot Access and Voting Integrity Initiative, which promised to “ma[ke] enforcement of election fraud and corruption offenses a top priority,” led to only 14 convictions of non-citizens for voting in three-year period. See Lorraine C. Minnite, *The Politics of Voter Fraud* at 8, Project Vote (Jan. 2007), [https://www.projectvote.org/wp-content/uploads/2007/03/Politics\\_of\\_Voter\\_Fraud\\_Final.pdf](https://www.projectvote.org/wp-content/uploads/2007/03/Politics_of_Voter_Fraud_Final.pdf).

by federal, state, and private entities.<sup>16</sup> The DHS SORN promises that information will be maintained as searchable case records for the next decade.<sup>17</sup> During that time, this information can be circulated to far-flung corners of the federal government for any number of purposes.<sup>18</sup> This alone risks chilling democratic participation by eligible individuals who simply do not trust the federal government’s possession and distribution of their sensitive information—especially where, as here, that information could be shared with private entities.<sup>19</sup> And it disregards the privacy interests of hundreds of millions of American voters. Only two weeks ago, a federal court evaluating a challenge to SAVE’s overhaul based on alleged violations of federal privacy law stated that the court “is troubled by the recent changes to SAVE and doubts the lawfulness of the Government’s actions.”<sup>20</sup> The court has expedited its consideration of the merits of the case “[g]iven the rapid ongoing developments and serious issues at stake.”<sup>21</sup>

Significantly for the undersigned Secretaries, SAVE’s expansion facilitates a dramatic and unwarranted encroachment by the executive branch into States’ power to run elections. The Department of Justice has confirmed that its demands for sensitive data contained in statewide voter registration lists seek to capitalize on SAVE’s increased capabilities.<sup>22</sup> The modifications to SAVE advance DOJ’s efforts to usurp Secretaries’ constitutional and statutory responsibility for voter-list maintenance, promote a false narrative of unchecked non-citizen voting, and rely on untested responses from disparate data sources to subject eligible voters to investigation and potential disenfranchisement.

---

<sup>16</sup> See DHS SORN at 48950-48951 (“Enumerators and Source Systems”); *id.* at 48953-48954 (“Record Source Categories”); Dep’t of Homeland Sec., *Privacy Impact Assessment for the Systematic Alien Verification for Entitlements “SAVE” Program* at 3-14 (Oct. 31, 2025) (“2025 SAVE PIA”), <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf>.

<sup>17</sup> DHS SORN at 48954-48955.

<sup>18</sup> DHS SORN at 48954 (“Routine Uses”).

<sup>19</sup> *Id.*; see also Part V, *infra*, describing SAVE’s proposed reliance on and incorporation of information from the National Law Enforcement Telecommunications System (NLETS), a seemingly private entity.

<sup>20</sup> Mem. Op. at 1, *League of Women Voters v. U.S. Dep’t of Homeland Sec.*, No. 1:25-cv-03501 (D.D.C. Nov. 17, 2025) (“LWV”), ECF No. 55, <https://www.courtlistener.com/docket/71499795/55/league-of-women-voters-v-us-department-of-homeland-security/>.

<sup>21</sup> *Id.* at 18; see also Joint Scheduling Proposal at 2, *LWV*, No. 1:25-cv-03501 (Nov. 21, 2025), ECF No. 57 (suggesting the parties be ordered to submit a scheduling proposal by January 9, 2026), <https://www.courtlistener.com/docket/71499795/57/league-of-women-voters-v-us-department-of-homeland-security/>.

<sup>22</sup> See, e.g., Jonathan Shorman, *DOJ is sharing state voter roll lists with Homeland Security*, Stateline (Sept. 12, 2025), <https://stateline.org/2025/09/12/doj-is-sharing-state-voter-roll-lists-with-homeland-security/>; Jonathan Shorman, *DOJ plans to ask all states for detailed voting info*, Stateline (Aug. 1, 2025), <https://stateline.org/2025/08/01/doj-plans-to-ask-all-states-for-detailed-voting-info/>; Sarah N. Lynch, *US Justice Dept considers handing over voter roll data for criminal probes, documents show*, Reuters (Sept. 9, 2025), <https://www.reuters.com/legal/government/us-justice-dept-considers-handing-over-voter-roll-data-criminal-probes-documents-2025-09-09/>.



## II. State election officials ensure well-maintained voter lists and free, fair, and secure elections.

In addition to being a significant and unlawful intrusion by the federal government into voters' privacy, SAVE also enables an impermissible intrusion by DHS and DOJ into the constitutionally assigned role to States and our offices to ensure and administer free, fair, and secure elections.

As the Supreme Court has recognized, even for federal elections, the “default,” is that States “have responsibility for the mechanics” of elections absent congressional action.<sup>23</sup> And even where the federal government can displace state rules, the U.S. Constitution “provides that Congress—not the President—is the check on States’ authority to regulate federal elections.”<sup>24</sup> In other words, the executive branch has no constitutional authority to unilaterally arrogate States’ election responsibilities to itself.

SAVE facilitates the executive branch’s continuing efforts to violate these constitutional boundaries. DHS’s and DOJ’s attempts to use SAVE to encroach on state authority is a particularly salient concern for the undersigned given DOJ’s recent demands of many States for unredacted copies of their statewide voter-registration lists<sup>25</sup> and President Trump’s demand that such lists be compared against federal databases for list-maintenance purposes.<sup>26</sup> It is clear that the expanded SAVE program is the next in a series of steps that the federal executive is taking to displace States’ authority—and, in turn, our offices’ role—over voter-eligibility determinations and list-maintenance activities.

Such a result would contradict the will of Congress, which has time and time again made clear that the States are responsible for ensuring that eligible voters, and only eligible voters, are registered to vote.

When it passed the NVRA, Congress sought to increase participation by eligible voters in federal elections, protect against discriminatory and unfair election laws and practices, promote the integrity of elections, and ensure accurate and current voter registration lists.<sup>27</sup> The Act established voter registration

---

<sup>23</sup> *Arizona v. Inter Tribal Council of Ariz., Inc.*, 570 U.S. 1, 9 (2013) (citation modified).

<sup>24</sup> *League of United Latin Am. Citizens v. Exec. Off. of the President*, 780 F. Supp. 3d 135, 194 (D.D.C. 2025) (explaining the import of the Elections Clause, U.S. Const. art. I, § 4).

<sup>25</sup> See Ali Swenson & Gary Fields, *The Justice Department seeks voter and election information from at least 19 states, AP finds*, Associated Press (Aug. 3, 2025), <https://apnews.com/article/justice-department-election-officials-voting-trump-a04b1522bed0cb6bbc286e25b139701f>; Press Release, Dep’t. of Justice, *Justice Department Sues Six States for Failure to Provide Voter Registration Rolls* (Sept. 25, 2025), <https://www.justice.gov/opa/pr/justice-department-sues-six-states-failure-provide-voter-registration-rolls>.

<sup>26</sup> Exec. Order No. 14248, 90 Fed. Reg. 14005, § 2(b)(iii) (Mar. 25, 2025), <https://www.govinfo.gov/content/pkg/FR-2025-03-28/pdf/2025-05523.pdf>.

<sup>27</sup> 52 U.S.C. § 20501.

requirements for federal elections, including registration through the state’s DMV, by mail, and via designated voter registration agencies.<sup>28</sup> And it imposed certain requirements on States to ensure that eligible applicants are registered to vote and to maintain accurate and current voter rolls, requirements the undersigned Secretaries consistently and regularly administer.<sup>29</sup>

In imposing these requirements, however, Congress imposed no documentary proof of citizenship requirement, and it required that any list-maintenance efforts ensure adequate safeguards for eligible voters. In connection with citizenship, Congress required only that registration materials for federal elections include a statement as to eligibility requirements, including citizenship, an attestation that the registrant meets those requirements, and the registrant’s signature under penalty of perjury.<sup>30</sup> Our offices follow these requirements and have implemented additional, reliable methods of ensuring accurate and current voter lists consistent with federal law.<sup>31</sup>

Similarly, HAVA established minimum standards that our offices follow in several key areas of administering elections for federal office.<sup>32</sup> These include maintenance of a single centralized computerized statewide voter list that includes the name and registration information of every legally registered voter in the State and that includes a unique identifier for them—that is, the voter’s valid driver’s license or state identification number, the last four digits of their SSN, or, for registrants without either, a specially assigned numeric identifier.<sup>33</sup> List maintenance is conducted consistent with the NVRA and HAVA<sup>34</sup> and includes coordination with other agency databases within the State.<sup>35</sup> Among other actions taken consistent with HAVA, the undersigned Secretaries verify the accuracy of the information that voter registrants provide against the state motor vehicle database

---

<sup>28</sup> 52 U.S.C. §§ 20503(a), 20504-20506.

<sup>29</sup> 52 U.S.C. § 20507.

<sup>30</sup> 52 U.S.C. §§ 20504(c)(2)(C), 20506(a)(6)(A), 20508(b)(2).

<sup>31</sup> See, e.g., Minn. Stat. § 201.161(1) (providing automatic voter registration only for those whose application includes “verification of United States citizenship or records reflect that the applicant provided proof of citizenship during a previous agency transaction”); Nev. Rev. Stat. § 293.5768(3)(b) (“An automatic voter registration agency shall not . . . [t]ransmit any information . . . if the person did not provide the agency in the normal course of business sufficient information that demonstrates the person is qualified to vote pursuant to NRS 293.485, including, without limitation, proof of identity, citizenship.”); Kristin Sullivan, *Automatic Voter Registration in Connecticut* at 2, 2017-R-0358, Connecticut General Assembly, Office of Legislative Research (Dec. 21, 2017), <https://www.cga.ct.gov/2017/rpt/pdf/2017-R-0358.pdf> (“The [memorandum of understanding] prohibits [the Department of Motor Vehicles] from electronically transmitting through the [automatic voter registration] system the records of individuals who . . . were issued a DMV credential but were not U.S. citizens at the time of issuance.”).

<sup>32</sup> 52 U.S.C. §§ 21081-21085.

<sup>33</sup> 52 U.S.C. § 21083(a).

<sup>34</sup> 52 U.S.C. § 21083(a)(2) (States exempt from the NVRA’s requirements remove names of ineligible voters consistent with state law).

<sup>35</sup> 52 U.S.C. § 21083(a)(1)(A)(iv).



and can maintain confidential agreements with the Commissioner of Social Security to determine whether an individual is shown on the SSA's records as deceased.<sup>36</sup>

At the same time that Congress imposed these requirements, it was careful to leave “[t]he specific choices on the methods of complying with [them] . . . to the discretion of the State[s].”<sup>37</sup> As to a voter’s citizenship, in particular, HAVA maintained the NVRA’s requirements and further specified that the form used for voter registration by mail in federal elections include two check boxes for the applicant to indicate whether they are a U.S. citizen and of voting age.<sup>38</sup> Congress included no further requirements.

Accordingly, the undersigned Secretaries—not the federal administration—are charged with responsibility for collecting voter registrants’ personal information, verifying their eligibility, registering them, maintaining voter registration lists, and administering state and federal elections.<sup>39</sup> We take these responsibilities very seriously, and execute them based on state-specific expertise we have developed over the course of decades. The use of SAVE to verify voter eligibility must remain voluntary and should only be used at the discretion of the election officials who have know-how to responsibly adopt and integrate list-maintenance procedures. And the federal executive cannot unlawfully seek state-maintained data to unilaterally submit to SAVE in search of non-citizen registrants. This would thwart state responsibility for list maintenance and create highly sensitive individualized records on millions of Americans in a manner that Congress did not authorize.

We also want to emphasize that, even as to voluntary use of SAVE, we will be hesitant to employ the system until DHS is transparent about the methods and standards used to establish reliability and we are convinced that SAVE produces reliable information and keeps possession of voters’ sensitive information with the States. If SAVE is not reliable—and, in fact, it currently appears to be unreliable—our use of SAVE would require us to undertake additional verification as to voters who overwhelmingly are likely to be eligible to vote, place unnecessary burdens on them, subject them to intrusive investigations, and possibly disenfranchise them. We are not willing to invite these results based on an unverified and largely untested system.

---

<sup>36</sup> 52 U.S.C. § 21083(a)(5)(B); *see also* 42 U.S.C. § 405(r)(9).

<sup>37</sup> 52 U.S.C. § 21085.

<sup>38</sup> 52 U.S.C. § 21083(b)(4)(A).

<sup>39</sup> *See, e.g., Smiley v. Holm*, 285 U.S. 355, 366 (1932) (States can regulate not only “times and places” but also “registration, supervision of voting, protection of voters, prevention of fraud and corrupt practices, counting of votes, duties of inspectors and canvassers, and making and publication of election returns”).

The undersigned Secretaries also are charged with safeguarding voters' personal information and ensuring compliance with state-law privacy protections.<sup>40</sup> Our willingness and ability to use SAVE turns on how well the data a State submits to SAVE is protected from disclosure, abuse, or potential misuse. It also turns on who ultimately retains possession of the resulting data. Here, we have serious concerns over the security and privacy of registered voters' personal information—information they entrusted to the State, not the federal government. While our offices often rely on data provided by others to ensure the accuracy and currency of our voter lists, we are unwilling to compromise voters' personal information by sharing it unnecessarily and without adequate safeguards and assurances. Indeed, our concerns related to SAVE currently far outweigh SAVE's utility to our offices. We discuss these concerns, and questions concerning SAVE's lawfulness, below.

### **III. The SORN raises grave privacy concerns, including compliance with the federal Privacy Act and State privacy obligations.**

What we currently know about SAVE triggers such grave privacy concerns that we doubt whether it is fit for use. We will not compromise the privacy and security of the personal information of would-be or registered voters, or risk unreasonably chilling participation by eligible voters. Indeed, SAVE's privacy encroachments are so significant that its use may be unlawful under basic privacy laws, including the federal Privacy Act and state-law privacy protections.

States have long and consistently protected voter privacy in their list-maintenance efforts. While our offices often rely on multiple data sources to maintain accurate and current voter lists, States historically have not provided the personal information of their voters to other agencies for list-maintenance purposes. Rather, our offices collect data from other sources and compare them to our lists. This approach is consistent with Congress's grant of authority over election administration—and, specifically, list maintenance—to the States, and it allows us to ensure compliance with both federal and state law.

Some States' participation in the Electronic Registration Information Center (ERIC) program, which provides state election officials with additional tools to

---

<sup>40</sup> *E.g.*, Minn. Stat. § 201.091, subd. 9 (“list[s] [of registered voters] provided for public inspection or purchase, or in response to a law enforcement inquiry, must not include a voter’s date of birth or any part of a voter’s Social Security number, driver’s license number, identification card number, military identification card number, or passport number”); Mich. Comp. Laws § 168.509gg(1)(c) (“The secretary of state, a designated voter registration agency, or a county, city, township, or village clerk shall not release a copy of that portion of a registration record [under the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246] that contains . . . [a] registered elector’s driver license or state personal identification card number.”); *id.* § 168.509gg(2) (“The last 4 digits of a registered elector’s Social Security number contained in a registration record may only be used by the secretary of state to verify a registered elector’s data as provided by the help America vote act of 2002 and to verify a registered elector’s status under this act, and must not be used or released for any other purpose.”).

maintain accurate and current voter lists, is the exception that proves the rule.<sup>41</sup> ERIC performs this function based on voter-registration and motor-vehicle data that member States submit to it, as well as official death data ERIC obtains from the SSA and official change of address data it obtains from the U.S. Postal Service.<sup>42</sup> The State-provided data is in encrypted files with a “cryptographic one-way hash” applied by the State “to sensitive data elements” that include the driver’s license or state ID number, any part of an SSN, and date of birth.<sup>43</sup> ERIC also uses additional information security and data security practices, there is no web-based access to ERIC’s servers, and ERIC’s members do not have access to any other member’s data.<sup>44</sup> In other words, while voter information is provided to ERIC, it is not vulnerable to unintended disclosure or misuse. Without the decryption key, the data is nothing more than “a string of random characters,”<sup>45</sup> and the key to decrypting the data is not held by any outside entity. And even the encrypted data shared externally is robustly protected.

Here, by contrast, SAVE both receives and retains personal information submitted for voter-verification purposes, including sensitive personal information that is readily identifiable.<sup>46</sup> Instead of “hashing” data like ERIC, for example, SAVE seemingly uses only “secure hypertext transfer protocol protected communications during all data transmission between the client workstation and the system.”<sup>47</sup> It then adds further information to individual records based on searches SAVE performs of federal, state, and other databases.<sup>48</sup> And it retains that enhanced file and makes it available for numerous other and future uses for at least ten years.<sup>49</sup> The DHS SORN states electronic records are “stored in a secure, cloud hosted environment,”<sup>50</sup> but it makes no mention of additional security features, such as hashing, meaning that sensitive personal data seemingly is accessible by those authorized to access the information—and anyone who gains unauthorized access.

---

<sup>41</sup> See Electronic Registration Information Center (ERIC), <https://ericstates.org> (last visited Nov. 26, 2025).

<sup>42</sup> ERIC, *Electronic Registration Information Center (ERIC): Technology and Security Overview* at 2 (Sep. 29, 2025), <https://ericstates.org/wp-content/uploads/documents/ERIC-Tech-Security-Brief.pdf>.

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

<sup>46</sup> DHS SORN at 48950-48951.

<sup>47</sup> 2025 SAVE PIA at 18, <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf>.

<sup>48</sup> DHS SORN at 48950-48953.

<sup>49</sup> DHS SORN at 48951, 48954-48955.

<sup>50</sup> DHS SORN at 48951; *see also* 2025 SAVE PIA at 17 n.22, <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf> (stating the “Verification Information System, including the services it houses, is in the Amazon Web Service cloud environment.”).

Unauthorized access is a significant and concrete risk given recent breaches and other incidents jeopardizing DHS data. In 2023, a data breach of the Homeland Security Information Network’s intelligence section (HSIN-Intel), DHS’s “official system for trusted sharing of Sensitive But Unclassified (SBU) information between federal, state, local, territorial, tribal, international and private sector partners,”<sup>51</sup> caused the entire system, including PII and sensitive information on election-related topics, to be accessible by tens of thousands of unauthorized users, including foreign governments and private contractors, for nearly two months.<sup>52</sup> A formal review by DHS concluded that the breach was caused by a DHS Intelligence and Analysis (I&A) developer who “inadvertently changed HSIN-Intel from a limited access group to an ‘everyone’ group - providing access to . . . all HSIN users, including those not approved for access to the HSIN-Intel.”<sup>53</sup>

And just this past summer, DHS was successfully targeted by two different hacking incidents—one in July, which was likely carried out by state-sponsored Chinese hackers who reportedly infiltrated DHS headquarters and several component agencies as part of a wider breach of Microsoft’s SharePoint service,<sup>54</sup> and another in August, which DHS itself described as “several severe lapses in security that allowed the threat actor to breach FEMA’s network and threaten the entire Department and the nation as a whole.”<sup>55</sup> DHS’s review of the 2023 data breach also “indicated that I&A’s privacy practices would benefit from additional

---

<sup>51</sup> See Dep’t. of Homeland Sec., *Homeland Security Information Network (HSIN)* (June 17, 2025), <https://www.dhs.gov/homeland-security-information-network-hsin>.

<sup>52</sup> Andy Greenberg, *A DHS Data Hub Exposed Sensitive Intel to Thousands of Unauthorized Users*, Wired (Sept. 16, 2025), <https://www.wired.com/story/a-dhs-data-hub-exposed-sensitive-intel-to-thousands-of-unauthorized-users/>.

<sup>53</sup> Memorandum to the Under Secretary of Intelligence and Analysis, from Intelligence Oversight Officer, *Preliminary Inquiry No. 2023-03 Factual Findings & Compliance Determination* at 1 (Feb. 28, 2024) (“DHS I&A Memo”), <https://www.brennancenter.org/media/14407/download/dhs-2023-03-report-and-mitigation.pdf?inline=1>.

<sup>54</sup> Margaret Brennan et al., *DHS and HHS among federal agencies hacked in Microsoft SharePoint breach*, CBS News (Jul. 24, 2025), <https://www.cbsnews.com/news/microsoft-sharepoint-breach-dhs-hhs/>; Renee Dudley, *Microsoft Used China-Based Engineers to Support Product Recently Hacked by China*, ProPublica (Aug. 1, 2025), <https://www.propublica.org/article/microsoft-sharepoint-hack-china-cybersecurity> (noting that “support for SharePoint is handled by a China-based engineering team that has been responsible for maintaining the software for years”).

<sup>55</sup> Press Release, Dep’t. of Homeland Sec., *Secretary Noem Terminates Inept FEMA Employees After Uncovering Massive Cyber Failures, Demands Accountability* (Aug. 29, 2025), <https://www.dhs.gov/news/2025/08/29/secretary-noem-terminates-inept-fema-employees-after-uncovering-massive-cyber>; see also *US Homeland Security chief reports breach at FEMA, fires 23 employees*, Reuters (Aug. 29, 2025), <https://www.reuters.com/world/us/us-homeland-security-chief-reports-breach-fema-fires-23-employees-2025-08-29/>.

clarification or training as to what constitutes U.S. Person Information (USPI) and/or Personally Identifiable Information (PII).”<sup>56</sup>

The privacy implications associated with SAVE’s use are particularly pronounced given how SAVE amasses voters’ personal information and leaves that information subject to possible misuse and abuse. Even where SAVE provides an initial response to a registered user that confirms a voter’s U.S. citizenship, DHS will maintain that voter’s personal information for the next decade.<sup>57</sup> This opens voters to security, privacy, and other risks and complications. SAVE is undoubtedly an attractive target for cyberattacks, and the possibility that the information contained within it will be spread across the federal government and to other recipients through “routine uses”<sup>58</sup> increases its vulnerability. Moreover, the federal administration will not ensure that members of the public are informed of the records SAVE maintains on them—or whether those records are shared across the government, provided to other recipients, and used for other purposes. Instead, SAVE places the burden on individuals to contact DHS with their sensitive personal information to obtain any information or access to records SAVE maintains on them.<sup>59</sup>

The DHS SORN and Privacy Impact Assessment do not adequately respond to our privacy concerns. Despite seeking to amass hundreds of millions of records with sensitive personally identifying information, they do not even commit to implement industry best practices as technology continues to rapidly evolve or to conduct regular security audits and evaluations of SAVE. Both the DHS SORN and the Privacy Impact Assessment simply reinforce significant concerns that our use of

---

<sup>56</sup> DHS I&A Memo at 2 (emphasis in original), <https://www.brennancenter.org/media/14407/download/dhs-2023-03-report-and-mitigation.pdf?inline=1>. This finding resulted in the recommendation and approval of a “Mitigation Measure” requiring the Director of the Transparency and Oversight Program Office to “prepare a message educating the I&A workforce on the differences between PII, SPII, and USPI.” See Memorandum to the Under Secretary of Intelligence and Analysis, from Acting Director, Transparency and Oversight Program Office, *Mitigation Recommendation for Preliminary Inquiry No. 2023-03* (May 9, 2024); Action to Acting Director, Transparency and Oversight Program Office, from Kenneth Wainstein, Under Secretary for Intelligence and Analysis, *Mitigation Measure for Preliminary Inquiry No. 2023-03* (May 9, 2024), <https://www.brennancenter.org/media/14407/download/dhs-2023-03-report-and-mitigation.pdf?inline=1>.

<sup>57</sup> DHS SORN at 48954-48955.

<sup>58</sup> DHS SORN at 48954.

<sup>59</sup> DHS SORN at 48955 (“Record Access Procedures” and “Contesting Record Procedures”). For would-be SAVE users who enter a memorandum of agreement with DHS, DHS seemingly places responsibility on user agencies to provide notice to individuals within their jurisdiction of their use of SAVE and makes users responsible for complying with federal and local authorities, including “factor[ing] the principles of notice, individual participation, and consent prior to providing information to [USCIS].” 2025 SAVE PIA at 20-21 (Oct. 31, 2025), <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf>.

the modified SAVE system would risk our citizens' privacy and conflict with federal and state law.

a. Federal Privacy Act

The modifications to SAVE raise serious questions under the Privacy Act, some but not all of which we discuss here.<sup>60</sup> SAVE promotes many of the things that the enactment of the Privacy Act sought to avoid—that is, the unnecessary and undisclosed collection, maintenance, and use by federal agencies of personal information on U.S. citizens and the unauthorized linking of electronic systems of records maintained by federal agencies.<sup>61</sup> As already noted, at least one federal court recently suggested that SAVE's overhaul may not be legal and has expedited its consideration of a challenge to the federal administration's actions.<sup>62</sup>

Significantly, the Privacy Act was enacted over 50 years ago in response to growing concerns about increasing computer usage and the adverse effects on individuals' privacy—concerns that remain highly relevant today and take on added significance in the context of highly sensitive personal information of America's registered voters. The Act principally governs federal agencies' collection, use, maintenance, and dissemination of individually identifiable information.<sup>63</sup> By recognizing individual privacy interests and setting limits on what information the federal government could retain on citizens, Congress sought for the Act to help restore public trust in the federal government after the Watergate and Counterintelligence Program scandals.<sup>64</sup>

The Act codified several important principles from a “code of fair information practices.”<sup>65</sup> These principles included allowing individuals to determine what records a federal agency maintained on them; requiring agencies to obtain consent before using an individual record collected for one purpose for other incompatible

---

<sup>60</sup> See 5 U.S.C. § 552a.

<sup>61</sup> See 5 U.S.C. § 552a note (“Congressional Findings and Statement of Purpose”), Pub. L. No. 93-579, § 2, 188 Stat. 1896 (Dec. 31, 1974), <https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf>; 5 U.S.C. § 552a note (“Construction of 1988 Amendments”), Pub. L. No. 100-503, § 9, 102 Stat. 2514 (Oct. 18, 1988), <https://www.congress.gov/100/statute/STATUTE-102/STATUTE-102-Pg2507.pdf>.

<sup>62</sup> Mem. Op. at 1, 18, LWV, No. 1:25-cv-03501 (Nov. 17, 2025), ECF No. 55, <https://www.courtlistener.com/docket/71499795/55/league-of-women-voters-v-us-department-of-homeland-security/>.

<sup>63</sup> For the Privacy Act, see 5 U.S.C. § 552a and its statutory notes. We focus primarily on the Privacy Act here, yet we recognize that other privacy-related statutes also govern the federal government's collection of personal information. These include, for example, the Paperwork Reduction Act, the E-Government Act, and the Federal Information Security Modernization Act. See 44 U.S.C. §§ 101 note, 3501 *et seq.*, 3551 *et seq.*, 3601 *et seq.*

<sup>64</sup> See U.S. Dep't of Just., Off. of Privacy and Civil Liberties, *Overview of the Privacy Act of 1974* at 1 (2020) (“OPCL Overview”), [https://www.justice.gov/Overview\\_2020/dl?inline](https://www.justice.gov/Overview_2020/dl?inline).

<sup>65</sup> *Id.*; see *Legislative History of the Privacy Act of 1974, Source Book on Privacy*, 94th Cong., 2d Sess. (Joint Comm. Print 1976), [https://www.justice.gov/d9/privacy\\_source\\_book.pdf](https://www.justice.gov/d9/privacy_source_book.pdf).



purposes; granting individuals a right of access to and an opportunity to amend inaccurate records pertaining to them; and directing agencies to collect such records only for lawful and authorized purposes and ensure their safety and integrity.<sup>66</sup> The principles are reflected in how federal agencies may collect, maintain, and secure information, in when they may make disclosures of individually identifiable information, and in what access and redress exists for individuals with respect to records pertaining to them.<sup>67</sup>

*Collection.* As relevant here, federal agencies must collect and maintain in their records systems only such information about an individual as is “relevant and necessary” to accomplish a statutorily recognized or other lawful purpose.<sup>68</sup> And agencies must ensure the “accuracy, relevance, timeliness, and completeness” of agency records used for individual determinations “as is reasonably necessary to assure fairness to the individual in the determination.”<sup>69</sup> These provisions generally have applied to eligibility determinations for public benefits or federal personnel actions.<sup>70</sup> But they are equally important in the context of voter eligibility. Where data will be used to determine whether an individual can exercise their right to vote or will be criminally investigated, they should have the right to expect that the data is, at a minimum, accurate, relevant, timely, and complete.

The Act also contains provisions governing when and how different federal agencies can match or link computerized information in their records systems. Congress amended the Privacy Act in 1988 to add provisions related to computer matching programs and impose corresponding procedural and due process requirements.<sup>71</sup> In so doing, it explained that the amendments were intended “to improve the oversight and procedures governing the disclosures of personal information in computer matching programs and to protect the privacy and due process rights of individuals whose records are exchanged in such matching programs.”<sup>72</sup>

The legislation responded to the “dramatic increase in the use of computer matching programs” by federal and state agencies and Congress’s recognition that, “unless adequately overseen and administratively controlled,” such programs “can pose significant risks to the due process and privacy rights of individuals.”<sup>73</sup> These risks could flow from “[t]he failure to verify the accuracy of the ‘hits’ produced by

---

<sup>66</sup> OPCL Overview at 1, [https://www.justice.gov/Overview\\_2020/dl?inline](https://www.justice.gov/Overview_2020/dl?inline).

<sup>67</sup> See, e.g., 5 U.S.C. § 552a(b)-(g), (i)-(k), (o)-(r).

<sup>68</sup> 5 U.S.C. § 552a(e)(1).

<sup>69</sup> 5 U.S.C. § 552a(e)(5).

<sup>70</sup> See, e.g., 5 U.S.C. § 552a(a)(8), (12), (13); § 552a(e), (o)-(p).

<sup>71</sup> See 5 U.S.C. § 552a(a)(8)-(13); § 552a(e)(12); § 552a(o)-(r), (u); OPCL Overview at 7 (also referencing further amendments in 1990 to 5 U.S.C. § 552a(p)), [https://www.justice.gov/Overview\\_2020/dl?inline](https://www.justice.gov/Overview_2020/dl?inline).

<sup>72</sup> S. Comm. on Governmental Affairs, *The Computer Matching and Privacy Protection Act of 1987*, S. Rep. No. 100-516, at 1, (2d Sess. 1988).

<sup>73</sup> *Id.* at 4, 6.

the matching program,” for instance, as well as being “subject to adverse actions solely on the basis of data that has been inadequately verified for accuracy.”<sup>74</sup> Risks also could arise from “the creation of permanent files or new systems of records from matching programs, because the existence of such ‘standing’ files of ‘hits’ from previous matches could too easily encourage the repeated use of these files for additional matching[]” and “pose[] serious threats to personal privacy” if not timely destroyed or governed by appropriate administrative, technical, and security procedures.<sup>75</sup> Although the definition of a “matching program” under the Act likely does not encompass SAVE’s use to verify voter eligibility, Congress emphasized in amending the Act that “[n]othing in the amendments . . . shall be construed to authorize,” among other things, “the establishment or maintenance by any agency of a national data bank,” “the direct linking of computerized systems of records maintained by Federal agencies,” “the computer matching of records not otherwise authorized by law,” or “the disclosure of records for computer matching except to a Federal, State, or local agency.”<sup>76</sup>

The modifications to SAVE raise serious questions under these statutory provisions and have been challenged in active federal court litigation. Through SAVE, DHS and DOJ seek to amass and maintain information on registered voters across the country, calling into question whether this is the de facto creation of a national voter registration database. Moreover, SAVE will accomplish this by assembling the search results of numerous other databases—overseen by both governmental and private entities—seemingly in violation of the Privacy Act.<sup>77</sup> DHS seemingly seeks to avoid application of the fair information principles and Privacy Act to SAVE by transferring to registered users many of the obligations it would have if Congress had actually authorized a matching program for voter eligibility verification purposes.<sup>78</sup> This merely reinforces the point that DHS likely is not maintaining SAVE consistent with federal law.

As to SSNs in particular, the Privacy Act requires a person’s disclosure of their SSN to be voluntary unless mandated for a specific purpose by federal

---

<sup>74</sup> *Id.* at 7-8.

<sup>75</sup> *Id.* at 16; *see also id.* at 16-17 (explaining the basis for requiring certain aspects to and procedures for matching agreements); 5 U.S.C. § 552a(o)(1)(F) (requiring “procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program”) and 5 U.S.C. § 552a(o)(1)(G) (requiring an agreement’s establishment of such controls).

<sup>76</sup> 5 U.S.C. § 552a(a)(8), 552a note (“Construction of 1988 Amendments”), Pub. L. No. 100-503, § 9, 102 Stat. 2514 (Oct. 18, 1988), <https://www.congress.gov/100/statute/STATUTE-102/STATUTE-102-Pg2507.pdf>; *see also* S. Rep. 100-516, at 10-14.

<sup>77</sup> DHS SORN at 48950-48953; 5 U.S.C. § 552a note (“Construction of 1988 Amendments”), Pub. L. No. 100-503, § 9, 102 Stat. 2514 (Oct. 18, 1988), <https://www.congress.gov/100/statute/STATUTE-102/STATUTE-102-Pg2507.pdf>.

<sup>78</sup> 2025 SAVE PIA at 16-22, <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf>; *see also* DHS SORN at 48952 (notably lacking any federal voting-related statutes among the “Authority for Maintenance of the System”).

statute.<sup>79</sup> Yet DHS seemingly envisions having SAVE assign SSNs to records that are submitted with only driver's license numbers.<sup>80</sup> When an election official submits a voter's driver's license or state identification card number to SAVE as their unique identifier, for example, SAVE may query state and private entities and attach a full SSN to that record even though the initial submission included no such information and the individual never voluntarily provided their SSN to either the election official or DHS.<sup>81</sup> Indeed, voter registrants are directed to provide a driver's license number before any SSN.<sup>82</sup>

In addition, and particularly as to its bulk processing feature and ability to ingest the contents of voter registration lists,<sup>83</sup> SAVE appears to invite violations of the Privacy Act's prohibition on maintaining records related to the exercise of First Amendment activity. The Act specifically prohibits a federal agency's maintenance of any record "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."<sup>84</sup> DOJ has demanded all fields of many States' voter lists, including voter history and political affiliation.<sup>85</sup> And it has confirmed that voter lists will be used in connection with SAVE.<sup>86</sup> To the extent that

---

<sup>79</sup> 5 U.S.C. § 552a note ("Disclosure of Social Security Number"), Pub. L. No. 93-579, §7, 88 Stat. 1909 (Dec. 31, 1974), <https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf>.

<sup>80</sup> DHS SORN at 48951 ("SAVE will use state driver's licensing agencies or another source (such as NLETS) to validate the information and gain access to other government enumerators. This will allow SAVE to match against other sources to verify immigration status and U.S. citizenship, which will improve accuracy and efficiency for SAVE user agencies.").

<sup>81</sup> *Id.*; see Decl. of Brian Broderick at 4, LWV, No. 1:25-cv-03501 (Oct. 22, 2025), ECF No. 37-1, <https://www.courtlistener.com/docket/71499795/37/1/league-of-women-voters-v-us-department-of-homeland-security/> (describing instances in which SAVE "captures . . . additional record information (full SSN, Alien number) and continues the automated query using additional accessed databases").

<sup>82</sup> 52 U.S.C. § 21083(a).

<sup>83</sup> DHS SORN at 48951 (explaining "*List Processor Feature*"); see also USCIS, News & Alerts, *SAVE Optimization: SAVE Enhances the Bulk Upload Process* (Jul. 21, 2025), <https://www.uscis.gov/save/current-user-agencies/news-alerts/save-optimization-save-enhances-the-bulk-upload-process>.

<sup>84</sup> 5 U.S.C. § 552a(e)(7).

<sup>85</sup> See, e.g., Letter from Harmeet K. Dhillon, Assistant Attorney General, to Shenna Bellows, Secretary of State of Maine, Re: Maine Voter Registration List with All Fields (Aug. 18, 2025), <https://www.maine.gov/sos/sites/maine.gov.sos/files/inline-files/DOJ%20State%20of%20Maine%20081825.pdf>; Letter from Harmeet K. Dhillon, Assistant Attorney General, to Jocelyn Benson, Secretary of State of Michigan, Re: Complete Michigan's Voter Registration List with All Fields (Aug. 14, 2025), [https://www.brennancenter.org/media/14701/download/michigan\\_08.14.2025\\_doj-letter.pdf?inline=1](https://www.brennancenter.org/media/14701/download/michigan_08.14.2025_doj-letter.pdf?inline=1); Letter from Harmeet K. Dhillon, Assistant Attorney General, to Justin R. Erickson, General Counsel, Re: Minnesota's Voter Registration List (Aug. 13, 2025), [https://www.brennancenter.org/media/14342/download/minnesota\\_08.13.25\\_doj-letter.pdf?inline=1](https://www.brennancenter.org/media/14342/download/minnesota_08.13.25_doj-letter.pdf?inline=1).

<sup>86</sup> See, e.g., Jonathan Shorman, *DOJ is sharing state voter roll lists with Homeland Security*, Stateline (Sept. 12, 2025), <https://stateline.org/2025/09/12/doj-is-sharing-state-voter-roll-lists-with-homeland-security/>.

all fields of the voter lists are imported into SAVE or logs with this information are kept within SAVE's system of records, this raises important First Amendment considerations, including whether the federal government, if it has ready access to this information, will inappropriately consider a voter's political affiliation, for example, in deciding whether to take certain action. It also heightens our concerns regarding the vulnerability of sensitive data collected through SAVE, as DHS's formal review of its 2023 data breach found that the breach included "43 improperly accessed products that touched on potentially sensitive topics from a privacy and civil liberties perspective such as election-related topics."<sup>87</sup>

*Disclosures.* The undersigned Secretaries are also acutely aware that, once a federal agency like DHS collects an individual's personal information, the Privacy Act contains many exceptions to the overarching principle of ensuring individual privacy.<sup>88</sup> These exceptions often will allow for disclosure of records that a federal agency possesses, including the voting-related data at issue here, whether it is personal information from voter lists that registered users submit to SAVE or additional information that SAVE attaches to those records, all of which then becomes available to numerous other persons and agencies. Depending on the circumstances, these further disclosures could include sharing individualized data with the DOJ, federal, state, and local law enforcement agencies, and even other registered users of SAVE that are federal, state, and governmental agencies—as the "Routine Uses" section of the SORN reflects.<sup>89</sup> As further explained below in Section V, this information could even end up with private entities that enable access to the data both domestically and internationally for law enforcement reasons—further raising the concern that SAVE's use runs afoul of Congress's directive that computer matching should not be construed to permit disclosure of personal information for matching beyond federal, state, and local agencies.<sup>90</sup>

Moreover, one of the two new "routine uses" the DHS SORN introduces again signals that the federal executive may seek to use SAVE to impermissibly intrude on the States' constitutionally recognized duties for administering state and federal elections, including list maintenance. In particular, the SORN highlights "*Auditing Verification Records To Support Oversight Organizations*" when discussing changes to SAVE.<sup>91</sup> Although not entirely clear, these three paragraphs seemingly reflect DHS's intent to share SAVE data, as individual case records and retrievable by

---

<sup>87</sup> DHS I&A Memo at 4, <https://www.brennancenter.org/media/14407/download/dhs-2023-03-report-and-mitigation.pdf?inline=1>.

<sup>88</sup> 5 U.S.C. § 552a(b).

<sup>89</sup> *Id.*; see DHS SORN at 48954.

<sup>90</sup> See Part V, *infra*, describing SAVE's proposed reliance on and incorporation of information from the National Law Enforcement Telecommunications System (NLETS), a seemingly private entity; see also 5 U.S.C. § 552a note ("Construction of 1988 Amendments"), Pub. L. No. 100-503, § 9, 102 Stat. 2514 (Oct. 18, 1988), <https://www.congress.gov/100/statute/STATUTE-102/STATUTE-102-Pg2507.pdf> ("Nothing in the amendments" to the Privacy Act "shall be construed to authorize . . . the disclosure of records for computer matching except to a Federal, State, or local agency.").

<sup>91</sup> DHS SORN at 48951; see also *id.* at 48954 (paragraph M).

state, with “[u]ser agencies with a legal authority to monitor and audit benefits granted *or voter registration records*.”<sup>92</sup> Under agreements they enter with DHS, such agencies “may view relevant case data such as biographic data, enumerators, case submission date/time, and SAVE response information” of individual user agencies and their case data and may view “other user agencies’ case data through a linking mechanism based on either benefit type granted (*e.g.*, Medicare) or by state.”<sup>93</sup> Other users will be able to “create cases within SAVE to verify applicants’ current eligibility for benefits previously granted” and ensure the agencies they monitor “are properly verifying immigration status or citizenship status before making an eligibility determination.”<sup>94</sup> The undersigned Secretaries are particularly interested in whether this “routine use” has been added, at least in part, to provide DOJ access to voter registration data States or their political subdivisions submit to SAVE. And even if not added specifically for this purpose, we would like DHS’s answer as to whether it will interpret this “routine use” to permit DOJ such access, which again raises significant issues of federal encroachment in addition to accuracy and privacy concerns.

In addition, DHS’s seeming ability to add new “routine uses” to information that already exists in SAVE presents the question of what it will next seek to do with the information SAVE retains. Our privacy concerns are compounded by what appears to be a retroactive application of new “routine uses” to information already in SAVE. Our offices apparently could submit queries to SAVE understanding the parameters of the system to be one thing only to confront changes to SAVE over the next decade that significantly alter the terms on which we provided registrants’ personal information to verify their voter eligibility. That is an unacceptable risk.

#### b. State Law Privacy Considerations

The undersigned Secretaries also must ensure the security and accuracy of the personal information on our voter rolls consistent with state law. State election and privacy laws impose obligations on us to protect voter information and other sensitive data. The way SAVE collects, stores, enhances, and further discloses a voter’s personal information is largely inconsistent with these responsibilities, which strictly limit the release of voter’s sensitive personal information and the uses of even redacted voter registration lists.

For example, California’s Election Code provides that a voter’s SSN, driver’s license number, and “any other unique identifier used by the State . . . for purposes of voter identification . . . are confidential and shall not be disclosed to any person.”<sup>95</sup> And California’s voter registration regulations place strict limitations on the Secretary and other election officials’ ability to release voter registration

---

<sup>92</sup> DHS SORN at 48951 (emphasis added).

<sup>93</sup> *Id.*

<sup>94</sup> *Id.*

<sup>95</sup> Cal. Elec. Code § 2194(b)(1); *see also* Cal. Gov’t Code § 7924.000(b) (same).

information to third parties, as well as the safeguards that must be employed by such third parties.<sup>96</sup> Likewise, under Maine, Oregon, Vermont, and Washington law, for example, data in the States' voter registration lists can only be released if the data is redacted to exclude personally identifying information, such as month and day of birth, SSN, and driver's license numbers.<sup>97</sup> And further, in Maine, all recipients of such data are prohibited from using "any part of the voter information for any purpose that is not directly related to activities of a political party, 'get out the vote' efforts[,] . . . or other activities directly related to a campaign."<sup>98</sup>

Similarly, in Minnesota, information about voters "provided for public inspection or purchase, or in response to a law enforcement inquiry, must not include a voter's date of birth or any part of a voter's Social Security number, driver's license number, identification card number, military identification card number, or passport number."<sup>99</sup> And in Michigan, the Secretary and other election officials "shall not release a . . . registration record [under the State's freedom of information act] that contains . . . [a voter's] driver license or state personal identification card number," and the last four digits of a voter's SSN "may only be used by the [S]ecretary . . . to verify a registered elector's data [and status] as provided by [HAVA and state law], and must not be used or released for any other purpose."<sup>100</sup>

In its Privacy Impact Assessment, DHS states that registered agencies are responsible for complying with federal and state law.<sup>101</sup> Indeed, DHS largely seeks to disclaim its responsibilities under federal law through its memoranda of agreement. Given the nature of SAVE's modifications, use of the system may well be inconsistent with federal and state law.

#### **IV. The SORN prompts significant concerns regarding the accuracy and reliability of SAVE data.**

The right to vote is protective of all other rights. Unsurprisingly, then, state and federal law are designed to ensure that procedures used to remove individuals from voter lists are nondiscriminatory,<sup>102</sup> and that no eligible voters are removed from the rolls because States use bad data sources to verify voter eligibility.<sup>103</sup> As

---

<sup>96</sup> See Cal. Code Regs. tit. 2, §§ 19005, 19008(a)(8), 19012, 19013.

<sup>97</sup> See Me. Rev. Stat. tit. 21-A, § 196-A(1)(B); Or. Rev. Stat. § 247.948(2); Vt. Stat. Ann. tit. 17, § 2154(b)(1); Wash. Rev. Code § 29A.08.710(2)(a).

<sup>98</sup> Me. Rev. Stat. tit. 21-A, § 196-A(1)(B)(1).

<sup>99</sup> Minn. Stat. § 201.091, subd. 9.

<sup>100</sup> Mich. Comp. Laws §§ 168.509gg(1)(c), 168.509gg(2).

<sup>101</sup> 2025 SAVE PIA at 16-22, <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf>.

<sup>102</sup> See 52 U.S.C. § 20507(b).

<sup>103</sup> See *id.* § 20507(a)(3) (providing registrants may not be removed except in certain circumstances); (c)(2)(A) (providing that States cannot systematically remove ineligible registrants within 90 days of a primary or general election for Federal office).



the stewards of our States’ voter lists, we are guided by twin principles relating to voter eligibility: Only eligible Americans may vote, but no eligible American should be denied the right to vote. This means that the data sources we use to verify voter eligibility must be trustworthy, and even where sources are trustworthy, we must verify the results.<sup>104</sup>

Bad data sources threaten voter eligibility, waste taxpayer resources, and prevent us from focusing verification efforts on accurate and reliable data sources. As a result, we must be selective about the data sources we use to verify our registration lists. In addition to having questions about SAVE’s legality and protection of voter data, Secretaries have reason to doubt the reliability and accuracy of SAVE’s responses—responses that the federal administration has signaled States should rely on in connection with a voter’s eligibility and citizenship status. In essence, by pushing States to use SAVE, the federal administration encourages reliance on a program that is still very much in development and risks depriving people of their constitutional right to vote and targeting them for criminal investigation. And the administration pushes SAVE’s use despite failing to provide testing data assuring States of its reliability—all while adopting legalese disclaiming responsibility for any unreliability in the data.<sup>105</sup>

DHS has not shown SAVE to be a reliable program the undersigned can treat as an acceptable data source that complies with federal and state law requirements for sources used in list maintenance. DHS has provided no information on how (or whether) it has tested the reliability of SAVE’s responses or any corresponding error rates, mismatches, or inconclusive responses. Nor has DHS provided information on the system’s accuracy based on the type of data submitted to the system (*e.g.*, name, address, date of birth, full SSN, last four digits of SSN, driver’s license number, or any combination of these) or certain voters’ characteristics (*e.g.*, a foreign-born citizen, a person who has changed their name, or a voter born before the SSA began systematically maintaining citizenship data with SSNs in 1981). The undersigned Secretaries therefore have no way to assess the reliability of the SAVE responses they would obtain based on any information they submit to SAVE, or

---

<sup>104</sup> Indeed, SAVE has always required significant verification efforts by the states to ensure a degree of accuracy. See U.S. Gov’t Accountability Off., GAO-17-204, Immigration Status Verification for Benefits: Actions Needed to Improve Effectiveness and Oversight 2 (Mar. 23, 2017), <https://www.gao.gov/assets/gao-17-204.pdf?inline=1>.

<sup>105</sup> DHS SORN at 48949 (“SAVE does not determine a benefit applicant’s eligibility for a specific benefit. Only the use agency makes that determination.”); 2025 SAVE PIA at 16-17, <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf> (explaining a registered agency’s memorandum of agreement with DHS/USCIS to use SAVE puts the obligation on the user to provide notice to those persons within their jurisdiction of their use of SAVE); *id.* at 19 (noting that “due to misspelling of names, transposed numbers, or incomplete information, the SAVE Program may produce inaccurate results”).

whether the use of the system is, for example, “uniform, [and] non-discriminatory” under federal law.<sup>106</sup>

There are significant reasons to question whether the changes to SAVE will produce accurate results. Historically, earlier versions of SAVE have proven to be of limited use to verify voter eligibility. The system of records only permitted searches of individuals who had been granted naturalized or derived U.S. citizenship or had a particular immigration status; it did not include U.S.-born citizens.<sup>107</sup> Running a search through earlier versions of SAVE thus required inputting a DHS-issued immigration-related identification number (something rarely collected as part of the voter registration process). DHS’s system also only allowed for individual inquiries, rather than bulk uploads of millions of records as SAVE now permits.<sup>108</sup> For all these reasons, many States doubted the usefulness of SAVE as part of their list-maintenance processes.<sup>109</sup> Indeed, previous DHS officials expressed concern over using SAVE for voter verification, as its information was “incomplete” and did “not provide comprehensive data on all eligible voters.”<sup>110</sup>

SAVE’s modifications attempt to address these limitations by enabling the bulk upload of voters’ information and combining disparate data sources held by different agencies. But combining data sources is notoriously challenging and requires careful evaluation before, during, and after records are linked. Before datasets can be merged, each source must be cleaned and standardized so that potential linkage fields (the pieces of information common to each dataset) are truly comparable. This includes addressing missing data, ensuring that fields capture the same attribute (e.g., distinguish legal from preferred names) and refer to the same point in time, resolving inconsistencies in naming conventions, capitalization, special characters, abbreviations, leading and trailing zeroes, whitespace, and other formatting differences. After assessing the quality of those fields, an appropriate

---

<sup>106</sup> 52 U.S.C. § 20507(b)(1).

<sup>107</sup> See Dep’t of Homeland Sec., *Privacy Act of 1974, System of Records*, 85 Fed. Reg. 31798, 31801 (2020); Dep’t of Homeland Sec., *Privacy Impact Assessment for the Systematic Alien Verification Entitlements Program* at 2 (June 30, 2020) (“2020 SAVE PIA”), <https://perma.cc/HU2M-NTL8>; see also DHS SORN at 48950 (describing this “expansion from the previous SAVE functionality, which limited U.S. citizenship verification to DHS records of naturalized and certain acquired U.S. citizens”).

<sup>108</sup> See 2020 SAVE PIA at 3-4; see DHS SORN at 48951 (describing bulk list processor feature).

<sup>109</sup> See, e.g., Virginia Dep’t of Elections, *Annual List Maintenance Report September 1, 2021-August 31, 2022*, at 8 (2022), <https://tinyurl.com/3u5xdttth> (“[I]t was ultimately determined that SAVE was unusable for list maintenance purposes due to limitations within the system.”). Before 2025, ten States had memorandums of understanding to use SAVE to verify the citizenship of voter registrants and eligible voters. See Fair Elections Ctr., *Eligible Voters at Risk: Examining Changes to USCIS’s Save System* at 1 (July 2025), <https://perma.cc/ZN5K-ATUC>. Not all were necessarily active users. See U.S. Comm’n on Civil Rights, *An Assessment of Minority Voting Rights Access in the United States* at 149 (Sept. 12, 2018), [https://www.usccr.gov/files/pubs/2018/Minority\\_Voting\\_Access\\_2018.pdf](https://www.usccr.gov/files/pubs/2018/Minority_Voting_Access_2018.pdf).

<sup>110</sup> Associated Press, *Feds OK Fla. access to citizens list*, Politico (Jul. 14, 2012), <https://www.politico.com/story/2012/07/feds-ok-fla-access-to-citizens-list-078507>.

matching method must be selected. When each dataset shares a reliable unique identifier, linking them is relatively straightforward. But when no universal unique ID exists across all data sources, as in this case, records must be matched using combinations of fields, such as first name, last name, and date of birth, and using different enumerator types, like full or partial SSN or state ID number, which increases the risk of both false positives (records incorrectly linked) and false negatives (records that should match but failed to).<sup>111</sup>

Once datasets are combined, the linkage must be evaluated through systematic quality checks, including reviewing match rates, identifying missed or incorrect matches, flagging duplicate matches, and diagnosing the sources of each type of error. Because no large-scale match is ever perfect, these checks are essential for understanding the reliability of the merged data.<sup>112</sup> Best practices require detailed documentation of each decision and assumption: how fields were cleaned, how matching rules were chosen, what error rates were observed, and which validated dataset served as the “source of truth” for evaluating false positives and false negatives. Clear reporting of the process, assumptions, and limitations is the only way for downstream users to interpret and assess the combined dataset appropriately.<sup>113</sup>

These reporting practices are especially critical because linkage quality can vary across demographic and socioeconomic groups. For example, a Census Bureau analysis found that racial minorities, lower income people, less educated people, residents of group quarters, more mobile people, and immigrants, including naturalized citizens, were harder to uniquely identify based on common data fields and thus harder to match across datasets.<sup>114</sup>

Separately, the added functionality of bulk processing of user-uploaded lists of individuals introduces an additional and significant source of potential error. Even if the underlying administrative databases in SAVE were perfectly matched, the system must then match those records to each individual in the bulk file, bringing all of the same challenges noted above, but compounded by the variability and unknown quality of the user-created bulk data. User-created bulk files may differ in formatting, completeness, time points, etc., and the system has no way to standardize these inputs. Further, these matches cannot be validated against a

---

<sup>111</sup> See Robert M. Goerge & Bong Joo Lee, *Matching and Cleaning Administrative Data*, in *Studies of Welfare Populations: Data Collection and Research Issues* 213, National Academies Press (2002), <https://www.nationalacademies.org/read/10206/chapter/9#212>.

<sup>112</sup> *Id.*

<sup>113</sup> See generally Mark Prell et al., *Transparent Reporting for Integrated Data Quality: Practices of Seven Federal Statistical Agencies*, FCSM 19-01, Fed. Comm. on Statistical Methodology (Sept. 2019), [https://nces.ed.gov/fcsm/pdf/Transparent\\_Reporting\\_FCSM\\_19\\_01\\_092719.pdf](https://nces.ed.gov/fcsm/pdf/Transparent_Reporting_FCSM_19_01_092719.pdf).

<sup>114</sup> Brittany Bond et al., *The Nature of the Bias When Studying Only Linkable Person Records: Evidence from the American Community Survey*, Working Paper #2014-08, CARRA Working Paper Series (Apr. 22, 2014), <https://www.census.gov/content/dam/Census/library/working-papers/2014/adrm/carra-wp-2014-08.pdf>.

data source that is a known “source of truth,” so any matching errors are effectively invisible.

Information provided by SSA itself underscores the basis for these concerns. SAVE will search SSA records systems, which SSA acknowledges “merely represent[] a snapshot of [an] individual’s citizenship status at the time of their interaction with SSA[.]”<sup>115</sup> Individuals report their citizenship status to SSA when they apply for an SSN and generally are not required to report a later change in their immigration status.<sup>116</sup> And many records lack even this “snapshot,” because SSA did not begin to consistently maintain citizenship information on issued SSNs until 1981.<sup>117</sup> Accordingly, an internal assessment reflected that approximately 25% of SSA’s records do not have an indication of citizenship present.<sup>118</sup> For these reasons, SSA admitted in litigation only a couple years ago that its records systems “do not provide definitive information about an individual’s citizenship status[.]”<sup>119</sup> Indeed, a 2006 SSA internal audit estimated that the Agency’s “citizenship data inaccurately identified about 3.3 million citizens as non-citizens ‘because they had become U.S. citizens after obtaining their SSN.’”<sup>120</sup> In other words, not all of SSA’s records of SSN holders reflect citizenship information and, even with respect to those that do, that information may be inaccurate. In the pending challenge to SAVE’s overhaul, DHS “[did] not dispute that such inaccuracies likely still exist.”<sup>121</sup>

Because SSA does not update citizenship status beyond an individual’s initial contact with the agency, naturalized citizens—who may become citizens after receiving an SSN but before registering to vote—undisputedly face a particularly high risk of being misidentified as non-citizens. But, as discussed above in connection with the Census Bureau’s analysis, other categories of registrants may also be vulnerable. We have no idea whether the same issues exist with SAVE, though its Privacy Impact Assessment acknowledges the risk of inaccurate results based on the misspelling of names, transposed numbers, or incomplete information.<sup>122</sup> The lack of testing and transparency around the modifications to

---

<sup>115</sup> Letter to Jon Sherman, Litigation Director & Senior Counsel, Fair Elections Center, from SSA Off. of Gen. Counsel, Re: Application for Records Testimony of a Social Security Administration (SSA) Employee in a Federal Civil Case, *Mi Familia Vota, et al. v. Adrian Fontes, in his official capacity as Arizona Secretary of State, et al.*, 22-cv-509 et al. (consolidated) (D. AZ) at 2 (Jul. 13, 2023), <https://perma.cc/KS2N-U2US>.

<sup>116</sup> *Id.*

<sup>117</sup> *Id.*

<sup>118</sup> *Id.* at 3.

<sup>119</sup> *Id.*

<sup>120</sup> Mem. Op. at 8, *LWV*, No. 1:25-cv-03501 (Nov. 17, 2025) (citing SSA Off. of the Inspector Gen., No. A-08-06-26100, Congressional Response Report: Accuracy of the Social Security Administration's Numident File iii (Dec. 18, 2006), <https://perma.cc/5G2JFF4V>), ECF No. 55, <https://www.courtlistener.com/docket/71499795/55/league-of-women-voters-v-us-department-of-homeland-security/>.

<sup>121</sup> *Id.*

<sup>122</sup> 2025 SAVE PIA at 19-20, <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf>.

SAVE and the reliability of SAVE's responses leaves us unsure about the extent of these disparate risks to voters, but there is ample cause for concern.

Underscoring our concerns about accurate and reliable data, accuracy failures in the system can be seen already in Travis County, Texas. Texas recently announced that it completed a "full comparison" between its voter registration list and SAVE.<sup>123</sup> Following this comparison, the Texas Secretary of State provided the results to the relevant counties so that the counties could "conduct their own investigations."<sup>124</sup> In the pending federal court litigation challenging SAVE's overhaul, Travis County's Voter Registration Director stated that about 25 percent of the "non-citizen matches" on his county's list had a voter source registration code indicating that they had "registered to vote at the Department of Public Safety (DPS) and, through the process at DPS, provided proof of citizenship at the time of registration."<sup>125</sup> Travis County's Voter Registration Director further noted that the Secretary of State's office could not clarify the issue and, more broadly, that he had "no visibility into how the [SAVE] matching process was conducted, how the list was created, or the reliability of the information within the database."<sup>126</sup> Travis County's experience also highlights that while SAVE's responses may be of uncertain quality and utility, they are certain to be a significant resource drain.

Nor is it clear who has responsibility for following up on initial responses from SAVE that call into question, or deem inconclusive, a voter's eligibility. The DHS SORN seems to place the burden on the registered user to request that DHS undertake "in-depth electronic and manual research in available records (including both electronic records as well as paper Alien Files (A-Files), when necessary[.]"<sup>127</sup> Yet DOJ and DHS represented in the pending federal court litigation that DHS will complete manual verification for inconclusive results related to voting-related queries without a further request.<sup>128</sup> In other words, the scope of the response a State will receive from SAVE when using the system to verify a voter's eligibility is not even clear. The need for clarity and controls around the additional verification DHS will undertake with respect to inconclusive results is a longstanding problem

---

<sup>123</sup> Press Release, Texas Sec'y of State, *Texas Completes Citizenship Verifications in the SAVE Database* (Oct. 20, 2025), <https://www.sos.state.tx.us/about/newsreleases/2025/102025.shtml>.

<sup>124</sup> *Id.*

<sup>125</sup> Decl. of Christopher Davis at 3, *LWV*, No. 1:25-cv-03501 (Oct. 29, 2025), ECF 47-1, <https://www.courtlistener.com/docket/71499795/47/1/league-of-women-voters-v-us-department-of-homeland-security/>.

<sup>126</sup> *Id.* at 2-3.

<sup>127</sup> DHS SORN at 48950 ("If SAVE is unable to provide an initial automated response verifying the benefit applicant's immigration status or U.S. citizenship, SAVE will provide instructions on actions the user agency may take, including requesting additional verification."); *id.* ("Users may also request additional verification when they have questions about a SAVE response or when requested by the benefit applicant.")

<sup>128</sup> *See* Decl. of Brian Broderick at 4, *LWV*, No. 1:25-cv-03501 (Oct. 22, 2025), ECF No. 37-1, <https://www.courtlistener.com/docket/71499795/37/1/league-of-women-voters-v-us-department-of-homeland-security/>.



for SAVE and one that predated its expansion. The Government Accountability Office reported in 2017 that USCIS lacked “sufficient controls to help ensure agencies are completing the necessary steps[.]”<sup>129</sup> The modifications to SAVE and the significantly expanded number of searches it entails may only exacerbate this issue and reduce the likelihood that DHS’s further verification is appropriately completed to ensure only the most accurate results.

## **V. DHS’s intent for SAVE to access DMV databases and NLETS highlights questions about SAVE’s privacy and reliability protections.**

The DHS SORN’s disclosure of DHS’s intent for SAVE to access State DMV databases and the National Law Enforcement Telecommunications System (NLETS) as record sources to verify an individual’s identity and to secure further enumerators highlights both our privacy and reliability concerns.<sup>130</sup> For the first time, the SORN provides for SAVE’s use of these data sources, in stark contrast to the record system’s previous reliance on record sources exclusively within or controlled by DHS. Yet the revised SORN does not even provide clarity regarding what the interchange of data with these external record sources will entail. And this interchange comes at a time when the federal administration is seeking to expand its use of NLETS for purposes beyond the targeted law enforcement for which it has historically been used, further supporting our concerns that an overarching purpose of SAVE is to amass private data on as many Americans as possible.<sup>131</sup>

The SORN’s discussion of NLETS is extremely limited, especially given that it is just one example of an entirely new and expansive *category* of record sources for SAVE: “state or national organizations issuing and maintaining driver’s license or state identification information *such as the NLETS*.”<sup>132</sup> Other than that disclosure, NLETS is mentioned only in a similarly cursory fashion in the SORN’s background section.<sup>133</sup> This background information suggests that SAVE will use voters’ identification numbers to access additional enumerators for them from NLETS. It is not clear how this would work in practice, and NLETS is not listed in the SORN under “Routine Uses” as a *recipient* of SAVE records. Yet the Privacy Impact

---

<sup>129</sup> U.S. Gov’t Accountability Off., GAO-17-204, Immigration Status Verification for Benefits: Actions Needed to Improve Effectiveness and Oversight 2 (Mar. 23, 2017), <https://www.gao.gov/assets/gao-17-204.pdf?inline=1>.

<sup>130</sup> DHS SORN at 48951, 48953.

<sup>131</sup> See Jonathan Shorman, *Homeland Security wants state driver’s license data for sweeping citizenship program*, Stateline (Nov. 25, 2025), <https://stateline.org/2025/11/25/homeland-security-wants-state-drivers-license-data-for-sweeping-citizenship-program/>.

<sup>132</sup> DHS SORN at 48953 (emphasis added).

<sup>133</sup> DHS SORN at 48951 (“By working with state driver’s licensing agencies and national agencies that store driver’s license information for legal purposes (such as the National Law Enforcement Telecommunications System (NLETS)), SAVE will use driver’s license and state identification card numbers to check and confirm identity information. When the agency provides a driver’s license or state identification card number as the enumerator to verify the identity of the applicant, SAVE will use state driver’s licensing agencies or another source (such as NLETS) to validate the information and gain access to other government enumerators.”).



Assessment DHS published in tandem with the SORN includes NLETS in a list of entities “[w]ith whom . . . personally identifiable information [will] be shared.”<sup>134</sup> Of particular concern is the fact that NLETS accesses data through automated computer requests, resulting in a lack of direct oversight regarding what data is shared and for what purpose.<sup>135</sup> Due to this and other concerns, some States are already restricting the transfer of their data using NLETS.<sup>136</sup>

The use of NLETS as a record source for SAVE is particularly concerning because, even though its leadership consists of State public safety officials, NLETS is a private entity not created or managed by any branch of government, state or federal. Instead, NLETS is a non-governmental, “international criminal justice and public safety information sharing hub,”<sup>137</sup> self-described as “the information superhighway of the law enforcement community.”<sup>138</sup> Indeed, its scale is staggering. NLETS apparently “connects over a million users, 800,000 devices and 45,000 agencies, making over 100 data sources available for them to query and share.”<sup>139</sup> But critically, NLETS “do[es] not own any of the data that is being used.”<sup>140</sup> This suggests that any data exchanged between SAVE and NLETS may be incorporated into one or more of the dozens of data sources NLETS relies on and then made available to over a million NLETS users, including over 30 corporate “strategic partners.”<sup>141</sup> The SORN does nothing to clarify the mechanics or ramifications of this arrangement.

The fact that NLETS is a tool of domestic and international law enforcement only exacerbates these concerns, especially if DHS intends to make data from SAVE available to numerous law enforcement agencies across different governmental levels, as well as “other appropriate authorit[ies].”<sup>142</sup> Under such an arrangement, the personally identifying information of registered voters who have perhaps never had any interaction with any arm of law enforcement could have their data integrated with numerous law enforcement databases that contain everything from vehicle registrations to biometric data. Even if we could assume that such

---

<sup>134</sup> 2025 SAVE PIA at 15-16, <https://www.dhs.gov/sites/default/files/2025-10/privacy-pia-dhsuscis006d-save-october2025%20%28002%29.pdf>.

<sup>135</sup> See Letters to Governors of Arizona, California, Colorado, Connecticut, Delaware, Hawaii, Kansas, Kentucky, Maine, Maryland, Michigan, New Jersey, New Mexico, North Carolina, Pennsylvania, Rhode Island, Wisconsin, Guam, and the U.S. Virgin Islands, from Members of the U.S. Congress at 2 (Nov. 12, 2025), <https://www.wyden.senate.gov/imo/media/doc/congressional-dmv-ice-letter-to-dem-governorspdf.pdf>.

<sup>136</sup> See *id.*

<sup>137</sup> Nlets, *Nlets History*, <https://nlets.org/about/history> (last visited Nov. 26, 2025).

<sup>138</sup> Nlets, *What We do*, <https://nlets.org/about/what-we-do> (last visited Nov. 26, 2025).

<sup>139</sup> Nlets, *10 Things You Might Not Know About Nlets* (Sep. 30, 2021), <https://nlets.org/resources/blog/10-things-you-may-not-know-about-nlets>.

<sup>140</sup> Nlets, *What We do*, <https://nlets.org/about/what-we-do> (last visited Nov. 26, 2025).

<sup>141</sup> Nlets, *10 Things You Might Not Know About Nlets* (Sep. 30, 2021), <https://nlets.org/resources/blog/10-things-you-may-not-know-about-nlets>.

<sup>142</sup> DHS SORN at 48954 (“Routine Uses”).

integration would be done securely and accurately—and we cannot—this use of voters’ information is completely outside of the realm of reasonable expectation when they registered to vote with their State or county elections office.

The undersigned Secretaries have profound concerns about allowing our citizens’ personal information to be used in such a sprawling and unrelated way without knowing more about what laws, if any, are applicable to and govern NLETS. We also need to more fully understand DHS’s use of NLETS and would want insight into any memoranda of understanding or other contractual obligations in place between DHS and NLETS; between NLETS and state, local, and federal law enforcement, justice, and public safety agencies; and between NLETS and its corporate partners. We find the SORN’s passing references to NLETS particularly alarming, given most people’s lack of familiarity with NLETS, its non-governmental status, and its domestic and international components.

## **VI. Conclusion**

There is no support for the claim that expansion of the SAVE program will give States access to a secure and accurate dataset for purposes of verifying voter eligibility. Indeed, DHS has not provided any information to show that the data matching in the SAVE program is reliable for purposes of voter-eligibility verification, nor demonstrated that its proposed uses of this data, including the 10-year retention period, are justified by law. What is apparent from the SORN, however, is that DHS is attempting to amass an unprecedented amount of private data on hundreds of millions of Americans to enable the federal government to usurp States’ constitutional authority. DHS should abandon this effort.

Sincerely,

A handwritten signature in blue ink, appearing to read "Shirley N. Weber".

Shirley N. Weber, Ph.D.  
Secretary of State  
California

A handwritten signature in blue ink, appearing to read "Stephanie Thomas".

Stephanie Thomas  
Secretary of the State  
Connecticut



William Francis Galvin  
Secretary of the Commonwealth  
Massachusetts



Shenna Bellows  
Secretary of State  
Maine



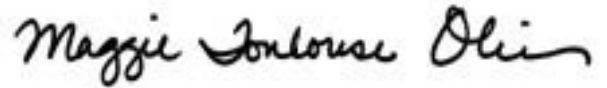
Jocelyn Benson  
Secretary of State  
Michigan



Steve Simon  
Secretary of State  
Minnesota



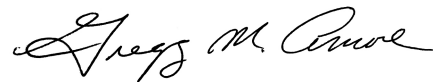
Lauren M. Zyriek  
Assistant Secretary of State  
New Jersey



Maggie Toulouse Oliver  
Secretary of State  
New Mexico



Tobias Read  
Secretary of State  
Oregon



Gregg M. Amore  
Secretary of State  
Rhode Island



Sarah Copeland Hanzas  
Secretary of State  
Vermont



Steve Hobbs  
Secretary of State  
Washington