UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

League of Women Voters, 1233 20th Street NW, Suite 500, Washington, DC 20036,

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

and

League of United Latin American Citizens, 1150 18th Street NW, Suite 650, Washington, DC 20036,

Plaintiffs,

v.

U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue SE, Washington, DC 20528**,**

Markwayne Mullin, in his official capacity as Secretary of Homeland Security, 2707 Martin Luther King Jr. Avenue SE, Washington, DC 20528,

U.S. Immigration and Customs Enforcement, 500 12th Street SW, Washington, DC 20024,

David J. Venturella, in his official capacity as Senior Official Performing the Duties of the Director of U.S. Immigration and Customs Enforcement, 500 12th Street SW, Washington, DC 20024,

Homeland Security Investigations, 500 12th Street SW, Washington, DC 20024,

John A. Condon, in his official capacity as Acting Executive Associate Director for Homeland Security Investigations, 500 12th Street SW, Washington, DC 20024,

COMPLAINT

Case No. 1:26-cv-3602

U.S. Citizenship and Immigration Services, 5900 Capital Gateway Drive, Camp Springs, MD 20746,

and

Joseph B. Edlow, in his official capacity as Director of U.S. Citizenship and Immigration Services, 5900 Capital Gateway Drive, Camp Springs, MD 20746,

Defendants.

INTRODUCTION

1. This case challenges the Department of Homeland Security's unlawful and secretive effort to compile voter records containing sensitive personal information about many of the nation's 174 million registered voters. DHS claims that it needs this information to identify voter fraud. But DHS has no authority to stockpile voter data for a nationwide election-law dragnet, and in carrying out this policy it has disregarded federal safeguards and violated the privacy rights of millions of Americans.

2. DHS's policy of collecting, maintaining, and using this information—the "Voter Data Collection Policy"—is the latest phase of the Trump-Vance administration's pursuit of alleged voter fraud. DHS has directed hundreds of agents to search voter records for supposed instances of noncitizens unlawfully registering or voting. In doing so, DHS has placed the data of nearly every American voter within the scope of its investigation.

3. The Voter Data Collection Policy is a massive invasion of privacy. DHS has obtained and is processing voter files from at least 47 states and has augmented those files with information purchased from commercial vendors. The resulting data set contains voting information and other personal data concerning millions of voters across the country.

4. The information DHS has amassed is highly sensitive. Depending on the state, it includes voters' Social Security numbers, driver's license numbers, dates of birth, addresses, phone numbers, race, sex, registration information, voting history, political-party affiliation, and other personal details.

5. DHS has implemented the Voter Data Collection Policy in secret. Only disclosures made in other litigation have provided any meaningful visibility into how DHS is acquiring millions of Americans' voter records or what it is doing with them. Even now, the public lacks key information about the policy's scope, operation, and safeguards.

6. Congress has imposed strict limits on the federal government's collection and maintenance of personal information, recognizing the government's vast information-gathering capacity and its power to affect individual lives. The Privacy Act permits an agency to maintain only information that is relevant and necessary to an authorized purpose and provides heightened protection for records concerning First Amendment activity.

7. Federal law also imposes transparency requirements designed to prevent misuse of sensitive data and to hold agencies accountable to the people whose privacy is at stake. Before establishing or revising a system of records, an agency must publish notice in the Federal Register, provide an opportunity for public comment when required, and issue a system of records notice ("SORN") describing the system and its uses. DHS has taken none of these required steps.

8. Furthermore, the Voter Data Collection Policy is unnecessary and wildly out of proportion to any legitimate objective. And, in any event, noncitizen voter fraud is not widespread. In centralizing records concerning voting—a core democratic activity bound up with the rights to free speech and association—the Voter Data Collection Policy contravenes the Privacy Act's restrictions on the collection of records concerning First Amendment activity.

9. The Voter Data Collection Policy is therefore an unlawful abuse of authority. Congress created DHS to prevent terrorism, secure the border, and address other specified threats—not to conduct a voter-fraud dragnet centered on the private voting information of millions of Americans and records reflecting the exercise of constitutional rights essential to democracy.

10. Plaintiffs bring this lawsuit to hold unlawful, vacate, set aside, and enjoin the Voter Data Collection Policy.

PARTIES

11. Plaintiff League of Women Voters ("LWV") is a nonprofit, nonpartisan, grassroots, community-based membership organization headquartered in Washington, D.C., that promotes

political responsibility by encouraging Americans to participate in the electoral process. Founded in 1920 as an outgrowth of the struggle to win voting rights for women, LWV now has more than a million members and supporters and is organized in nearly 800 communities and in every state and the District of Columbia. LWV comprises two entities: the League of Women Voters of the United States ("LWVUS") and the League of Women Voters Education Fund ("LWVEF"). LWVUS is a 501(c)(4) social welfare organization that encourages informed and active participation in government, works to increase understanding of major public policy issues, and influences public policy through education and advocacy. LWVEF is a 501(c)(3) organization and works to register and provide voters with election information through its election resource VOTE411.org, candidate forums, and debates.

12. As part of its mission, LWV, along with its state and local Leagues—its affiliate organizations—operates one of the longest-running and largest nonpartisan voter registration efforts in the nation. Through its work, LWV registers many thousands of voters every election cycle and is instrumental in ensuring access to voter registration for all eligible voters, including naturalized and derived U.S. citizens.

13. Plaintiff Electronic Privacy Information Center ("EPIC") is a nonprofit organization headquartered in Washington, D.C., that was established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC believes that all people deserve protection from abusive data practices like mass surveillance, browser tracking, demographic profiling, and data discrimination. Central to EPIC's mission is oversight and analysis of government activities that impact individual privacy, freedom of expression, and democratic values.

14. EPIC is a membership organization. An individual member of EPIC is any person who contributes to the advancement of EPIC's mission, who acts in accordance with the core values

and policies of EPIC, and who has been recognized and registered as a member by EPIC, by virtue of payment of annual dues or having been granted a dues waiver. This includes members of EPIC's Advisory Board, who are distinguished experts in law, technology, and public policy.

15. Plaintiff League of United Latin American Citizens ("LULAC") is a nationwide, non-profit, nonpartisan, membership-based organization with 359 councils (chapters) and 896,972 members nationwide. LULAC was established in 1929 and is headquartered in Washington, D.C.

16. LULAC is the largest and oldest Latino civil rights organization in the United States. Its mission is to improve the lives of Latino families throughout the United States and to protect their civil rights through community-based programs in each of its 359 councils.

17. LULAC's members include both U.S.-born citizens and naturalized citizens. Its members are civically engaged: Approximately 83% are registered to vote, nearly 76% of LULAC's registered members voted in 2020, and around 62% voted in 2022, exceeding the voting rates of the general population.

18. Throughout the year, LULAC's members, working through its councils, register prospective voters and hold voter registration drives at naturalization ceremonies, schools, churches, and other community events. At these events, LULAC members, working through its councils, often, at the request of registrants, collect voter registration forms and return them to local election offices in accordance with state law. LULAC holds get-out-the-vote programs before elections to encourage its members to vote.

19. Defendant U.S. Department of Homeland Security ("DHS") is a federal agency. DHS is headquartered in Washington, D.C. DHS is an agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), the Paperwork Reduction Act ("PRA"), 44 U.S.C. § 3502(1), and the Administrative Procedure Act ("APA"), 5 U.S.C. § 551(1).

20. Defendant Markwayne Mullin is the Secretary of Homeland Security and is sued in his official capacity.

21. Defendant U.S. Immigration and Customs Enforcement ("ICE") is a federal law enforcement agency within DHS. ICE is headquartered in Washington, D.C. ICE is an agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), the PRA, 44 U.S.C. § 3502(1), and the APA, 5 U.S.C. § 551(1).

22. Defendant David J. Venturella is the Senior Official Performing the Duties of the Director of ICE and is sued in his official capacity.

23. Defendant Homeland Security Investigations ("HSI") is a federal law enforcement agency within ICE and DHS. HSI is headquartered in Washington, D.C. HSI is an agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), the PRA, 44 U.S.C. § 3502(1), and the APA, 5 U.S.C. § 551(1).

24. Defendant John A. Condon is Acting Executive Associate Director for HSI and is sued in his official capacity.

25. Defendant U.S. Citizenship and Immigration Services ("USCIS") is a federal agency within DHS. USCIS is headquartered in Maryland. USCIS is an agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), the PRA, 44 U.S.C. § 3502(1), and the APA, 5 U.S.C. § 551(1).

26. Defendant Joseph B. Edlow is the Director of USCIS and is sued in his official capacity.

JURISDICTION

27. This Court has jurisdiction under 28 U.S.C. § 1331 because this action arises under the laws of the United States. This Court has further remedial authority under the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202, and the Administrative Procedure Act, 5 U.S.C. § 701 *et seq*.

VENUE

28. Venue lies in this District under 28 U.S.C. § 1391(e)(1)(A) and (C) because Defendants include officers and agencies of the United States headquartered in this District and at least one Plaintiff resides in this District.

LEGAL BACKGROUND

29. Congress has recognized that federal agencies' collection, maintenance, and use of sensitive information carry serious risks, including to personal privacy. For that reason, agencies must comply with federal laws—including the Privacy Act and the Paperwork Reduction Act—that spell out how and when agencies may gather and maintain such information.

Privacy Act

30. Congress enacted the Privacy Act "in the wake of the Watergate and the Counterintelligence Program (COINTELPRO) scandals involving illegal surveillance on opposition political parties and individuals deemed to be 'subversive.'"[1] In passing the law, Congress "sought to restore trust in government and to address what at the time was seen as an existential threat to American democracy."[2] In particular, the Privacy Act reflected congressional "concern over 'the impact of computer data banks on individual privacy.'"[3]

31. The Privacy Act places sharp procedural and substantive limits on how federal agencies may collect and use personal information. In many cases, these limits are more stringent than those applicable to private actors.

---

[1] U.S. Dep't of Just., *Overview of the Privacy Act of 1974*, at 1 (2020 ed.), https://perma.cc/6SB9-XAEK.

[2] *Id.*

[3] *U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press*, 489 U.S. 749, 766 (1989) (quoting H.R. Rep. No. 93-1416, at 7 (1974)).

32. The Privacy Act sweeps broadly and imposes those limits whenever an agency "maintains a system of records." 5 U.S.C. § 552a(e).

33. Under the Act, a "system of records" is a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *Id.* § 552a(a)(5).

34. A record, in turn, is defined as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." *Id.* § 552a(a)(4).

35. Finally, to "maintain" a record or a system of records means to "maintain, collect, use, or disseminate" that record or system. *Id.* § 552a(a)(3).

36. The Privacy Act limits *what information* an agency may maintain. Agencies that maintain a system of records must "maintain . . . only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." *Id.* § 552a(e)(1).

37. Moreover, agencies must "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." *Id.* § 552a(e)(5).

38. When information concerns the First Amendment activity of individuals, the Privacy Act imposes "an even more rigorous standard."[4] Agencies may not "maintain" any "record describing how any individual exercises rights guaranteed by the First Amendment unless expressly

[4] Privacy Act Guidelines—July 1, 1975, 40 Fed. Reg. 28949, 28965 (July 9, 1975).

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." 5 U.S.C. § 552a(e)(7).

39. The Privacy Act also requires agencies to take *specific steps* before collecting or maintaining new information. Upon the "establishment or revision" of any system of records, the agency must publish in the Federal Register a notice—known as a "system of records notice" or "SORN"—containing detailed information about the system, including:

a. the system's "name and location," *id.* § 552a(e)(4)(A);

b. "the categories of individuals" whose records are maintained, the "categories of records maintained," and the "categories of sources of records," *id.* § 552a(e)(4)(B)–(C), (I);

c. "each routine use of the records . . . including the categories of users and the purpose of such use," *id.* § 552a(e)(4)(D);

d. agency "policies and practices" for the records, *id.* § 552a(e)(4)(E); and

e. procedures allowing an individual to be notified "if the system of records contains a record pertaining to him," to "gain access" to such a record, and to "contest its content," *id.* § 552a(e)(4)(G)–(H).

40. Moreover, if a SORN will propose a new or intended use of records in a system of records, the agency must do more than merely publish the SORN: It must engage in a period of notice and comment beforehand. Specifically, at least 30 days before releasing the SORN, the agency must publish a separate notice in the Federal Register identifying the "new use or intended use of the information in the system" and must "provide an opportunity for interested persons" to comment. *Id.* § 552a(e)(11).

41. Thus, "[a]ny new or significantly modified routine uses require a minimum of 30 days after publication in the Federal Register before the routine uses are effective." Off. of Mgmt. & Budget ("OMB") Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and*

Publication under the Privacy Act, at 7 (2016), https://perma.cc/N9QK-SDLE. And agencies "shall" review and consider any "public comments on a published SORN." *Id.*

Paperwork Reduction Act

42. The Paperwork Reduction Act ("PRA") complements the Privacy Act by providing additional protection against the collection of Americans' personal information. Specifically, one of the statutory purposes of the PRA is to "ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to . . . privacy and confidentiality, including [the Privacy Act]." 44 U.S.C. § 3501(8)(A).

43. The PRA outlines a comprehensive process that agencies must comply with before engaging in any "collection of information."

44. The Act defines a "collection of information" to include "the obtaining, causing to be obtained, [or] soliciting . . . of facts or opinions by or for an agency, regardless of form or format, calling for . . . answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States." *Id.* § 3502(3)(A)(i).

45. For the purposes of the PRA, a "person" includes "an individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision." *Id.* § 3502(10).

46. Before engaging in any collection of information, the PRA mandates that agencies undertake a rigorous process involving input from inside and outside of government.

47. First, agencies must conduct a review of the proposed collection of information, which must include an evaluation of need, a description of the information sought, plans for the collection

and use of that information, and "a specific, objectively supported estimate of burden." *Id.* § 3506(c)(1)(A); *see also id.* § 3507(a)(1)(A).

48. Second, agencies must provide 60-day notice in the Federal Register and solicit public comment on, among other things, the necessity of, and burden imposed by, the collection of information. *Id.* § 3506(c)(2)(A). Agencies must also consult with other affected agencies. *Id.*

49. Third, agencies must evaluate the public comments they receive. *Id.* § 3507(a)(1)(B).

50. Fourth, agencies must "certify (and provide a record supporting such certification . . .) that each collection of information" is necessary, non-duplicative, reduces burden to the extent practicable, and meets other criteria. *Id.* § 3506(c)(3). The certification must be submitted to OMB. *Id.*; *see also id.* § 3507(a)(1)(C).

51. Fifth, agencies must issue a notice in the Federal Register indicating that they have submitted the proposed collection to OMB. *Id.* § 3507(a)(1)(D). After that notice, OMB must wait at least 30 days for a second period of public comment before deciding whether to approve the collection of information. *Id.* § 3507(b).

52. Sixth, agencies must obtain the approval of OMB and procure from OMB a control number to be displayed upon the collection of information. *Id.* § 3507(a)(2)–(3).

53. If the agency fails to take any of these steps in advance, it "shall not conduct or sponsor the collection of information." *Id.* § 3507(a).

FACTUAL ALLEGATIONS

Statewide Voter Registration Lists

54. Under federal law, each state must maintain an official, centralized list of every legally registered voter in the state. *See* 52 U.S.C. § 21083(a)(1)(A).[5] While the exact contents of these

[5] North Dakota is exempt from this requirement under a grandfather provision. *See id.* § 21083(a)(1)(B).

statewide voter registration lists ("SVRLs") vary from state to state, they always include the name of each registered voter. *Id.* The lists also typically include the voter's address. Depending on the state, the lists frequently include sensitive personal information, such as race, sex, date of birth, date of registration, phone number, complete or partial Social Security number, driver's license number, voting history, and political party affiliation.

55. SVRLs are commonly used by political parties and candidates for electoral purposes. Every state allows at least some requesters to obtain some voter registration information under at least some circumstances.

56. But many states place restrictive limits or conditions on the release of information in voter files. Many states charge a fee—in some jurisdictions, up to thousands of dollars—to obtain voter information.[6] Other states prohibit requests for voter files for commercial purposes. *See, e.g.*, N.H. Rev. Stat. Ann. § 654:31(VI). Some states restrict who can request the files, limiting their release to, for instance, political parties and candidates, government entities, law enforcement agents, and other narrowly drawn groups. *See, e.g.*, Cal. Elec. Code § 2194(a).

57. South Carolina, for example, states that "[y]ou must be a registered South Carolina voter to purchase a list."[7]

58. Massachusetts only makes its voter rolls available to "state party committees, statewide candidate committees, state ballot question committees, the jury commissioner, adjutant general and any other individual, agency or entity that the state secretary shall designate by regulation." Mass. Gen. Laws ch. 51, § 47C.

---

[6] *See, e.g.*, Wis. Election Comm'n, *Badger Voters: Frequently Asked Questions*, https://perma.cc/5SCL-TLRN.

[7] S.C. Election Comm'n, *Sale of Voter Registration Lists*, https://perma.cc/CL4W-UDMF; *see also* S.C. Code Ann. § 7-3-20(D)(13).

59. States also place restrictions on the sorts of information that can be released. For example, states typically do not authorize the disclosure of Social Security numbers and driver's license numbers to members of the public, even where those numbers are otherwise contained in SVRLs. *See, e.g.*, Ga. Code Ann. § 21-2-225(b).

60. Although states are in charge of policing their voter rolls, federal law imposes further limitations. For example, a federal statute declares it "unlawful for any alien to vote in any election held solely or in part for the purpose of electing a candidate for the office of President, Vice President, Presidential elector, Member of the Senate, Member of the House of Representatives, Delegate from the District of Columbia, or Resident Commissioner." 18 U.S.C. § 611(a).[8]

61. Congress has authorized the Department of Justice ("DOJ") to enforce federal election laws. *See, e.g.*, 28 U.S.C. §§ 516, 519; 52 U.S.C. § 10308.

Trump-Vance Administration's Efforts to Combat Alleged Voter Fraud

62. The Trump-Vance administration has prioritized combatting alleged voter fraud in federal elections, and has specifically focused on unsubstantiated claims of widespread noncitizen voter fraud. In pursuit of that priority, the Trump-Vance administration has endeavored to unlawfully collect and maintain sensitive voter registration lists.

63. On March 25, 2025, President Trump signed Executive Order 14248, "Preserving and Protecting the Integrity of American Elections," which directed the Attorney General to "prioritize enforcement of 18 U.S.C. [§§] 611 and 1015(f) and similar laws that restrict non-citizens from registering to vote or voting." Exec. Order No. 14248, § 2(e), 90 Fed. Reg. 14005, 14007 (Mar. 28, 2025). It also directed the Attorney General, along with the DHS Secretary, to take measures

[8] A judge in the Southern District of Florida recently held this statute to be unconstitutional because, with few inapplicable exceptions, "Congress has no power to say *who can* vote or *who cannot* vote in federal elections." *United States v. Cox*, No. 0:25-CR-60249, 2026 WL 2948729, at *1 (S.D. Fla. Oct. 1, 2026).

to identify—or ensure that states could identify—unqualified voters on state registration rolls. *Id.* § 2(b)(i), (e)–(f).

64. Following the Executive Order, in May 2025, the Department of Justice began issuing letters to states insisting that they produce complete SVRLs, which include sensitive personal information about registered voters, as detailed above. At least 48 states and the District of Columbia have received such demands, and many have refused to comply.[9]

65. DOJ has sued 30 states and the District of Columbia for non-compliance, resulting in litigation in multiple jurisdictions continuing to the present day.[10] So far, DOJ has lost every case decided. More than 20 district courts have rejected DOJ's demands for complete SVRLs, and one circuit court has affirmed a district court's judgment. In contrast, *no* federal court has ordered a state to comply with DOJ's demands for SVRLs.[11] For example, a district court in Georgia recently dismissed yet another of these lawsuits. *See* Order, *United States v. Raffensperger*, No. 1:26-cv-00485 (N.D. Ga. Sep. 30, 2026), Dkt. No. 146.

66. However, at least 16 states have voluntarily provided, or said they would provide, their complete, unredacted SVRLs to DOJ.[12] Those unredacted SVRLs include highly sensitive personal information like driver's license numbers and partial or complete Social Security numbers that states typically do not disclose to members of the general public.

67. Other states have provided DOJ, or offered to provide DOJ, with a publicly available version of their SVRLs that they offer to individuals entitled to request the files under state law.[13]

---

[9] Kaylie Martinez-Ochoa et al., *Tracker of Justice Department Requests for Voter Information*, Brennan Ctr. for Just. (Aug. 24, 2026), https://perma.cc/BZL9-5VVA.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

68. On March 6, 2026, Todd M. Lyons, then the Senior Official Performing the Duties of the Director of ICE, sent a letter to Harmeet K. Dhillon, the Assistant Attorney General for Civil Rights. In the letter, Lyons requested, pursuant to the Privacy Act, 5 U.S.C. § 552a(b)(7), that DOJ "provide HSI with the public Statewide Voter Registration Lists (SVRLs) in its possession, in order for HSI to conduct appropriate investigation of potential violations of federal election law."[14]

69. On March 12, 2026, DOJ responded to that letter, confirming that "[a]fter DHS signed the appropriate DOJ-CRT [DOJ Civil Rights Division] Use Agreement on March 12, 2026, DOJ-CRT granted the appropriate DHS counterpart access to the data via DOJ-CRT's secure file-sharing system," and agreeing to further "coordinate the exchange of records maintained by [HSI] that are necessary to carry out an authorized law enforcement activity by the DOJ in which the Department of Homeland Security (DHS) may rely on routine use provisions in its applicable SORN(s) to share."[15] The March 12 letter also states that DHS indicated to DOJ that DHS has the "ability and intent to enrich the SVRL datasets with DHS records to allow for vetting via the SAVE system."[16]

70. On May 12, 2026, DOJ's Office of Legal Counsel ("OLC") issued an opinion (the "OLC Opinion") stating that DOJ's Civil Rights Division "has authority to seek statewide voter lists and share them with the Department of Homeland Security as part of its effort to identify individuals who are ineligible to vote."[17]

---

[14] Letter for Harmeet K. Dhillon, Assistant Attorney General for Civil Rights, from Todd M. Lyons, Senior Official Performing the Duties of the Director of ICE (Mar. 6, 2026), *included in* Administrative Record, *Common Cause v. U.S. Dep't of Just.*, No. 1:26-cv-01352, at CRT-0003398 (D.D.C. July 2, 2026), Dkt. No. 45-7.

[15] Letter for Todd M. Lyons, Senior Official Performing the Duties of the Director of ICE, from Eric V. Neff, Acting Chief of the Voting Section, Civil Rights Division, Department of Justice (Mar. 12, 2026), *included in* Administrative Record, *Common Cause v. U.S. Dep't of Just.*, No. 1:26-cv-01352, at CRT-0003399 (D.D.C. July 2, 2026), Dkt. No. 45-7.

[16] *Id.*

[17] *Authority to Obtain and Share Statewide Voter Roll Data*, 50 Op. O.L.C. __, at *1 (May 12, 2026), https://perma.cc/HL2E-SQKQ.

71. The OLC Opinion addresses both HSI's authority to obtain the files and its compliance with the Privacy Act.

72. The OLC Opinion concedes that it is an "admittedly close[] question" whether "HSI is authorized by law to investigate such voter fraud."[18]

73. OLC also states that although the Privacy Act "authorizes disclosure for law-enforcement purposes," such disclosure (1) must be "for a civil or criminal law enforcement activity" that "is authorized by law," and (2) "the head of the agency or instrumentality" must have "made a written request" that meets certain requirements.[19] Specifically, under the Privacy Act, the written request must specify "the particular portion desired and the law enforcement activity for which the record is sought." 5 U.S.C. § 552a(b)(7).

74. The OLC Opinion does not identify a system of records in which HSI—or any other component of DHS—intends to store SVRLs.

75. On July 16, 2026, President Trump delivered a nationally televised address from the White House claiming that United States elections are highly vulnerable to election fraud, including infiltration by noncitizen voters, and that our country is experiencing a "crisis of election security."[20] He cited what he called "a stunning investigation by the Department of Homeland Security," which he said "identified approximately 278,000 non-citizens who are registered to vote in federal elections" from "state voter rolls and public records."[21] The President claimed that "the real number is actually much higher than that," and blamed a lack of proof on certain states'

---

[18] *Id.* at *37.

[19] *Id.* (quoting 5 U.S.C. § 552a(b)(7)).

[20] Zachary B. Wolf & Annette Choi, *Trump's Speech Claiming US Election Vulnerabilities, Annotated*, CNN (July 17, 2026), https://perma.cc/CD6W-AHBQ.

[21] *Id.*

"refus[al] to share their voter files."[22] According to President Trump, "these disclosures reveal an election system so broken and so vulnerable that no one can possibly defend it."[23]

76. At a news conference the next day, Secretary Mullin expanded on President Trump's accusation of widespread noncitizen voter fraud, prefacing his remarks with a warning that President Trump only "hit the highlights, and those should be scary for everybody."[24] The Secretary specified that DHS had "identified 250,000 noncitizens registered to vote in just four states"—California, Pennsylvania, New Jersey, and Nevada.[25] And he posted on Twitter/X that he had "put these governors on notice," attaching letters he had sent to secretaries of state in the implicated jurisdictions requesting that they respond within two weeks.[26]

77. But the attached letters, in contrast to President Trump's and Secretary Mullin's public pronouncements, caveated the findings as only a "[p]reliminary review" revealing that there "may be" that many unlawful voters, indicating that the numbers the administration had touted might not be accurate.[27]

78. And in fact, they were not.

79. Within weeks, inferior DHS officials were forced to admit that they could not deliver proof of President Trump's and Secretary Mullin's public accusations of noncitizen voter fraud as to at least one of the states that Secretary Mullin had identified.

---

[22] *Id.*

[23] *Id.*

[24] Sebastian Murdock, *DHS Secretary Helps Spin Trump's 2020 Election Lies*, HuffPost (July 17, 2026), https://perma.cc/9HDX-KZCY.

[25] Amy Sherman & Louis Jacobson, *Fact-Checking the Trump Administration's Count of 250,000 Noncitizens on the Voter Rolls*, PolitiFact (July 17, 2026), https://perma.cc/2MPR-36LQ.

[26] Secretary Markwayne Mullin (@SecMullinDHS), X (July 17, 2026, at 1:37 PM), https://perma.cc/N9CE-DMY7.

[27] *Id.*

80. During a mid-August meeting with election officials from Nevada, a state in which Secretary Mullin had claimed DHS identified 15,903 noncitizens registered to vote, DHS officials admitted that they had identified just 185.[28]

81. When Nevada investigated those 185 individuals, it found that every single one of them was a U.S. citizen.[29]

82. DHS also failed to deliver proof of the allegations against California, Pennsylvania, and New Jersey.[30]

83. At the same July 17 press conference in which he announced inflated totals of voter fraud violations, Secretary Mullin also claimed that DHS had identified 400,000 deceased voters on state voter rolls.[31]

84. Recently, DHS has launched what it refers to as the "Unlawful Voter Initiative." Under that initiative, DHS is redirecting USCIS agents to a nationwide effort to identify noncitizens who have illegally voted or registered to vote. The initiative relies on the data of voters from across the country, most of which originated in SVRLs. Agents are instructed to check this voter information against other federal databases listing citizenship and immigration information to identify possible

---

[28] Nick Corasaniti, *Homeland Security Made a Big Claim About Noncitizen Voting. Now It Can't Prove It.*, N.Y. Times (Aug. 20, 2026), https://perma.cc/2999-VP26.

[29] Nick Corasaniti, *From 16,000 to 185 to Zero: Trump's Claims of Illegal Voting in Nevada Fizzle*, N.Y. Times (Sep. 24, 2026), https://perma.cc/G7F5-X6SK.

[30] Jude Joffe-Block & Miles Parks, *DHS Acknowledges the Noncitizen Numbers It Touted on Voter Rolls Were Inflated*, NPR (Aug. 25, 2026), https://perma.cc/3ST9-H4L7; Robert Farley, *Trump Overstates Magnitude of Noncitizen Voting in New Jersey*, FactCheck.org (Aug. 5, 2026), https://perma.cc/KB5Q-84RP.

[31] Rebecca Beitsch, *Mullin Threatens States as DHS Launches Widespread Review of Elections*, The Hill (July 17, 2026), https://perma.cc/WGP9-HM4M.

instances of voter fraud. Cases of potential fraud are referred to HSI for further review and investigation.[32]

Voter Data Collection Policy

85. Defendants decided on and implemented a policy—the "Voter Data Collection Policy"—to collect, maintain, augment, and use available SVRLs to support DHS's efforts to identify purported instances of voter fraud.

86. Further, DHS itself has made clear that its efforts are not limited to immigration enforcement and criminal investigations of alleged non-citizen voters. For example, DHS has taken it upon itself to examine supposedly deceased voters.[33] In its own words, DHS's efforts are broadly aimed at "election integrity" and "protect[ing] the lawful voting process."[34]

87. The "strategic direction" of the Voter Data Collection Policy is to employ a "network-based investigative approach, prioritizing organization and facilitation analysis over individual leads."[35]

88. Internal DHS documents reflect that DHS's priorities include a "voter fraud agenda" focused on "voter rolls clean up" and reviewing "2020 results."[36]

---

[32] Nick Corasaniti & Hamed Aleaziz, *Trump Administration Begins Blitz to Find Elusive Voter Fraud Ahead of Midterms*, N.Y. Times (Sep. 2, 2026), https://perma.cc/K3LZ-MWSK.

[33] Rebecca Beitsch, *Mullin Threatens States as DHS Launches Widespread Review of Elections*, The Hill (July 17, 2026), https://perma.cc/WGP9-HM4M.

[34] *See, e.g.*, ICE Memorandum for HSI Executive Leadership, *Re: Fraud Related Investigative Activity and Accomplishments* (June 2026), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 034); HSI Election Integrity Investigations at 1 (May 25, 2026), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 055). DHS provided this and other information cited in the complaint in heavily redacted form in response to Freedom of Information Act litigation. *See Democracy Forward Found. v. U.S. Dep't of Homeland Sec.*, No. 26-cv-02624 (D.D.C.).

[35] Email from Chief of Staff, Countering Transnational Organized Crime, HSI (May 26, 2026, at 12:28 PM), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 125).

[36] HSI Voter Fraud Agenda, *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 046–47).

Acquisition and Scale of the Voter Data

89. According to an internal government email dated September 1, 2026, as a part of the Voter Data Collection Policy, DHS has obtained some version of the SVRLs of at least 47 states.[37]

90. Some of the SVRLs in DHS's possession were obtained by HSI from DOJ pursuant to the agreement described above between DOJ and ICE.[38]

91. Other SVRLs came to HSI through Heather Honey, the DHS Deputy Assistant Secretary for Election Integrity, from unspecified sources.[39]

92. USCIS also says it has received "voter information through a variety of sources, including, but not limited to, information voluntarily provided by state and local jurisdictions, publicly available information, and other lawfully available data."[40]

93. DHS has received and processed massive amounts of data. An internal HSI report on "HSI Election Integrity Investigations" dated June 1, 2026—which DHS produced in heavily redacted form in response to a Freedom of Information Act ("FOIA") request—states that HSI had "ingested" "50.6 million records" in a "DOJ Dataset Intake," with "[p]riority states includ[ing] Texas, Pennsylvania, California, New Jersey, Minnesota, Michigan, Arizona, Florida, Georgia, and Ohio."[41]

---

[37] Kristina Cooke & Peter Eisler, *White House Pushes for Speedy Review of Voter Rolls in Hunt for Noncitizen Voters*, Reuters (Sep. 24, 2026), https://perma.cc/D347-SKR8.

[38] HSI Election Integrity Investigations at 4 (June 1, 2026), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 131).

[39] *Id.*

[40] Decl. of Nicolas Bartell, *Cal. Nurses Ass'n v. Mullin*, No. 4:26-cv-10680, ¶ 10 (N.D. Cal. Sep. 28, 2026), Dkt. No. 46-1.

[41] HSI Election Integrity Investigations at 4 (June 1, 2026), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 131).

94. The June 1, 2026 HSI report also describes a "DHS Dataset Intake" of "48.4 million records [that] were obtained by [Deputy Assistant Secretary] Heather Honey through independent sources of information."[42]

95. USCIS also contributed to this effort. The June 1, 2026 HSI report states that HSI "[p]rioritiz[ed] 26,563 USCIS-derived records for downstream vetting" and has "[d]isseminated . . . 1,586 [leads] to 24 HSI field offices."[43]

96. As the Director of DOJ's Office of Privacy and Civil Liberties recognized, DHS's acquisition of this "huge amount of raw unprocessed voter registration data" carried significant "legal risk, given that 99% of the data would implicate the privacy and civil liberties of United States Citizens."[44]

97. An internal HSI report dated August 31, 2026—which DHS produced in litigation in heavily redacted form—indicates that HSI is currently engaged in a "50 State Voter Roll Processing" effort.[45]

98. The SVRLs in HSI's possession do not just include narrowly targeted information about suspected noncitizen voters. Rather, the SVRLs contain data for *every single voter* on a given state's voter rolls.

Data Enrichment and Integration

99. DHS has aggregated (or, in DHS's preferred term, "enriched") the SVRLs in its possession with information purchased from commercial databases like Accurint, a data tool developed by

---

[42] *Id.*

[43] *Id.*

[44] Peter Elkind et al., *Inside Trump's Failed Hunt for Noncitizen Voters*, ProPublica (Aug. 14, 2026), https://perma.cc/X2NY-CW42.

[45] HSI Election Integrity Investigations (Aug. 31, 2026), *included in* Administrative Record, *Cal. Nurses Ass'n v. Mullin*, No. 4:26-cv-10680, at AR-2-001 (N.D. Cal. Sep. 29, 2026), Dkt. No. 50-2.

LexisNexis and used by law enforcement.[46] This "[d]ata [e]nrichment" effort is being carried out, at least in part, by HSI's Innovation Lab ("iLab").[47]

100. The commercial data used by DHS often include highly sensitive information like driver's license numbers and Social Security numbers. Accordingly, DHS's "[e]nrichment" efforts have allowed it to maintain this highly sensitive information on voters even where the SVRLs standing alone would not reveal such information. For example, according to a recent disclosure from a DHS whistleblower, DHS has used data from Accurint to fuse data on Connecticut voters with those voters' Social Security numbers.[48]

101. But even the "enriched" SVRLs do not include citizenship data for voters and are not limited to suspected noncitizen voters.

102. A July 6, 2026 report from HSI describes the status of "iLab State Processing" and explains that voter files from Missouri, Michigan, New Mexico, Connecticut, Georgia, and Kentucky "have been enriched by the iLab."[49]

103. According to the DHS whistleblower disclosure, DHS employees were informed that additional data on voters were also to be added through "supplemental magic."[50]

---

[46] Kristina Cooke & Peter Eisler, *White House Pushes for Speedy Review of Voter Rolls in Hunt for Noncitizen Voters*, Reuters (Sep. 24, 2026), https://perma.cc/D347-SKR8; Declaration of Nicolas Bartell ¶ 10, *Cal. Nurses Ass'n v. Mullin*, No. 4:26-cv-10680 (N.D. Cal. Sep. 28, 2026), Dkt. No. 46-1.

[47] HSI Election Integrity Investigations at 4 (June 1, 2026), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 131).

[48] Letter for the Honorable Alex Padilla, U.S. Senator, from Norman L. Eisen, Executive Chair, Democracy Defenders Fund, & Stephen A. Jonas, Chief Counsel & Director, Rapid Response Legal, Democracy Defenders Fund, app. at 16 (Sep. 8, 2026) ("Whistleblower Disclosure Letter"), https://perma.cc/MK8U-JP2X.

[49] HSI Election Integrity Investigations at 1 (July 6, 2026), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 140).

[50] Whistleblower Disclosure Letter at 3, app. at 19.

Operational Use and Enforcement Consequences

104. DHS is using the SVRLs it has amassed under the Voter Data Collection Policy to feed its Unlawful Voter Initiative. DHS agents, including ICE and USCIS agents, are trawling through SVRLs to match individual voters' data against other federal data sources containing citizenship and immigration information with the goal of identifying potential instances of supposed voter fraud.[51] DHS has used this data to target not only noncitizens but also U.S. citizens—on the theory that naturalized citizens may have unlawfully voted or registered to vote before naturalizing.[52] Additionally, as part of its dragnet, DHS is necessarily accessing and scrutinizing lawfully registered voters' data, which make up the overwhelming majority of entries in the SVRLs.

105. HSI has also sought to load the SVRLs it has amassed into its enforcement systems. A May 26, 2026 internal HSI email from an HSI official states that "iLab's processing focuses on DOJ voting rolls and USCIS data," and that "[c]oordination with iLab continues, particularly on ingesting processed voter roll data into the ELITE enforcement system to enhance lead management, analytical review, and investigative tracking."[53] "ELITE" is a tool created by the technology company Palantir and is used by DHS to identify—and in some cases locate—targets for ICE operations.[54]

---

[51] Kristina Cooke & Peter Eisler, *White House Pushes for Speedy Review of Voter Rolls in Hunt for Noncitizen Voters*, Reuters (Sep. 24, 2026), https://perma.cc/D347-SKR8; Whistleblower Disclosure Letter app. at 1.

[52] Whistleblower Disclosure Letter app. at 22.

[53] Email from Chief of Staff, Countering Transnational Organized Crime, HSI (May 26, 2026, at 12:28 PM), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 125).

[54] Joseph Cox, *'ELITE': The Palantir App ICE Uses to Find Neighborhoods to Raid*, 404 Media (Jan. 15, 2026), https://perma.cc/GG75-R9YH.

106. HSI has also worked to supplement its SVRLs with criminal history information. As that same May 26 email describes, "criminal histories are currently excluded" from iLab's processing, but "efforts [are] underway to address this."[55]

107. HSI has identified "voter roll acquisition" and "data enrichment" as "cent[ral]" to the agency's efforts to combat election fraud.[56]

108. On October 13, 2026, DOJ sent a letter to the California Secretary of State highlighting Secretary Mullin's claim that "there are likely numerous noncitizens registered to vote in the federal election in California."[57] The letter demanded that California review a list of "people the Federal Government believes are likely noncitizens who were sent a vote-by-mail ballot to participate in the November 2026 federal election" within 48 hours and take action to prevent ineligible voters from voting.[58] The letter instructed California to comply with DOJ's demand by "contacting election@hq.dhs.gov"—an email address belonging to DHS, not DOJ.[59]

109. On October 15, 2026, DOJ sued California, alleging that California illegally sent mail ballots to voters "without verifying citizenship in collaboration with the Federal Government."[60] The complaint claims that "[b]ased on a thorough analysis of voter rolls and federal data, agencies within the Department of Homeland Security found thousands of likely noncitizens registered to

---

[55] Email from Chief of Staff, Countering Transnational Organized Crime, HSI (May 26, 2026, at 12:28 PM), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 125).

[56] *See, e.g.*, HSI Election Integrity Investigations at 1 (June 15, 2026), *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 029).

[57] Letter for Shirley N. Weber, California Secretary of State, from R. Trent McCotter, Acting Deputy Attorney General at 1 (Oct. 13, 2026), *available at* https://perma.cc/TVU7-KDJY.

[58] *Id.*

[59] *Id.* at 2.

[60] Complaint, *United States v. California*, No. 2:26-cv-12025, ¶ 5 (C.D. Cal. Oct. 15, 2026), Dkt. 1.

vote in California who would automatically be sent federal ballots under State law."[61] The complaint also asserts that "USCIS regularly conducts investigative processes whereby lists of registered voters or information about voters on voter rolls are analyzed" to identify voter fraud and that "California's voter roster containing voter registration information is made available for purchase."[62] The complaint also states that "[i]n some situations, a state voter file is sent to HSI before it is sent to USCIS."[63] And it notes that "USCIS utilizes third-party software" to analyze voter data.[64]

110. DOJ's letter to California and its subsequent lawsuit demonstrate that DHS possesses voter files for California and other states and is using those files for election administration purposes.

Accuracy Failures and False Positives

111. DHS is incapable of accurately identifying instances of voter fraud based on SVRLs. The systems and data sources DHS relies on to check the citizenship status of voters contain numerous errors and regularly produce false positives that incorrectly suggest that U.S. citizens have voted illegally.

112. For example, DHS has compared voter files with iLab data to identify instances of voter fraud. As one iLab staffer explained, however, that process generates "an 'ungodly' number of false positives."[65] Staff at the iLab viewed this method of comparison as "a little insane."[66] When

---

[61] *Id.* ¶ 3.

[62] *Id.* ¶ 33.

[63] *Id.* ¶ 41.

[64] *Id.* ¶ 35.

[65] Peter Elkind et al., *Inside Trump's Failed Hunt for Noncitizen Voters*, ProPublica (Aug. 14, 2026), https://perma.cc/6VZG-UKY8.

[66] *Id.*

DHS compared Pennsylvania and New Jersey voter data with iLab data, for instance, the result was the significantly inflated count of voter fraud violations that DHS identified earlier this summer.[67]

113. In addition, DHS has used data from the Systematic Alien Verification for Entitlements ("SAVE") system to identify alleged voter fraud. That system, as modified in 2025, amalgamates citizenship and immigration data from the Social Security Administration ("SSA") and other sources. The modified SAVE system was designed to, among other purposes, allow state agencies to check whether individuals listed on their voter rolls are not U.S. citizens and thus are ineligible to vote.

114. The SAVE system and the SSA data it contains are incapable of accurately verifying a person's status as a U.S. citizen and an eligible voter. As one judge in this district has held at summary judgment, "the modified SAVE has caused inaccurate rather than accurate matching of citizenship data." *League of Women Voters v. U.S. Dep't of Homeland Sec.*, 835 F. Supp. 3d 79, 135 (D.D.C. 2026) (citing record evidence), *stayed on other grounds sub nom. U.S. Dep't of Homeland Sec. v. League of Women Voters*, No. 26A308, 2026 WL 2879700 (U.S. Sep. 25, 2026). DHS itself has recognized that "[s]hortfalls in data accuracy in the system could cause . . . false results."[68]

115. Nevertheless, DHS continues to use the SAVE system "to further DHS law-enforcement functions" and "help determine whether illegal voting may have occurred."[69]

---

[67] *Id.*

[68] DHS, *Privacy Threshold Analysis for the SAVE Program* 17 (July 17, 2025), https://perma.cc/9AXY-WCLU.

[69] Notice, *League of Women Voters v. U.S. Dep't of Homeland Sec.*, No. 1:25-cv-03501 (D.D.C. Sep. 14, 2026), Dkt. No. 146; Decl. of Nicolas S. Bartell, *League of Women Voters v. U.S. Dep't of Homeland Sec.*, No. 1:25-cv-03501, ¶¶ 3–4 (D.D.C. Sep. 14, 2026), Dkt. No. 146-2.

116. DHS is aware of the impossibility of reliably identifying instances of voter fraud by cross-matching voter file information with citizenship information in its possession. In an internal email, a DHS official admitted that the agency only had "some degree of confidence" that the individuals the Unlawful Voter Initiative has flagged had actually "registered to vote and/or voted" unlawfully.[70]

117. Under the Unlawful Voter Initiative, where DHS flags an individual as an unlawful voter, it creates a "TECS" record for that individual.[71] The creation of a TECS record can lead to significant consequences. For instance, the existence of a TECS record regarding an individual may cause that individual to be subjected to additional screening at the border.[72] It can also result in loss of eligibility for "trusted traveler" programs like Global Entry, which enable expedited processing at airports and other ports of entry.[73]

118. According to the DHS whistleblower disclosure, "DHS source data is not reliable enough to justify creating a TECS record" and DHS's process "is knowingly sweeping known US citizens in as potentially 'unlawful voters.'"[74]

---

[70] Kristina Cooke & Peter Eisler, *White House Pushes for Speedy Review of Voter Rolls in Hunt for Noncitizen Voters*, Reuters (Sep. 24, 2026), https://perma.cc/D347-SKR8.

[71] Whistleblower Disclosure Letter at 2–3, app. at 14. Under an earlier version of the system, TECS stood for "Treasury Enforcement Communications System." As used today, however, TECS is not an acronym.

[72] Whistleblower Disclosure Letter at 3; DHS, *Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing* at 12 (Dec. 22, 2010), https://perma.cc/Q7RD-6KQK.

[73] GAO, *Trusted Traveler Programs: DHS Has Enrollment Processes, but CBP Should Provide Additional Information on Reconsiderations* 15–16 & n.23, 49 (Feb. 2024), https://perma.cc/QT6L-EVJS; 8 C.F.R. § 235.12(b)(2)(iv).

[74] Whistleblower Disclosure Letter app. at 24.

119. The Voter Data Collection Policy allows DHS to expand the reach of its Unlawful Voter Initiative. The policy will result in DHS inaccurately identifying more U.S. citizens as having unlawfully voted and incorrectly creating TECS records in their name.

Failure to Comply with Procedural Requirements

120. In implementing the Voter Data Collection Policy, Defendants have not taken the procedural steps that the Privacy Act requires an agency to engage in before collecting and maintaining this type of data.

121. Defendants did not publish a SORN in connection with their collection, maintenance, and use of SVRLs, or the data used to "enrich" the SVRLs.

122. Defendants did not publish a notice of a new or intended use of information in connection with their collection, maintenance, and use of SVRLs, or the data used to "enrich" the SVRLs.

123. Defendants did not solicit comments on a new or intended use of information or evaluate such comments.

124. Defendants have failed to adhere to the PRA's preconditions for conducting a collection of information.

125. Defendants have not conducted a review as described by the PRA, including an evaluation of need, a description of the information, plans for the collection and use of the information, and a specific, objectively supported estimate of burden.

126. Defendants have not solicited or evaluated public comments on any PRA review.

127. Defendants have not submitted to OMB a certification regarding the collection of information.

128. Defendants have not provided a second period of notice and comment regarding the collection of information.

129. Defendants have not obtained final approval from OMB for the collection.

Injuries to Plaintiffs

130. Plaintiffs LWV, EPIC, and LULAC—and the members of each Plaintiff—have suffered and are continuing to suffer privacy injuries as a result of the Voter Data Collection Policy.

131. LWV, EPIC, and LULAC each have members who reside and vote in jurisdictions where DHS maintains voter files pursuant to the Voter Data Collection Policy.

132. For example, LWV, EPIC, and LULAC each have members in California, New Jersey, Nevada, Pennsylvania, Washington, Wisconsin, Missouri, Georgia, New York, Connecticut, and Minnesota—11 states that DHS has singled out for its voter fraud efforts. HSI recently announced a "coordinated criminal voter fraud surge initiative" targeting nine of those states: California, Nevada, Pennsylvania, Washington, Wisconsin, Missouri, Georgia, New York, and Connecticut.[75] Moreover, DHS has previously alleged, without evidence, that across four of those states—California, New Jersey, Nevada, and Pennsylvania—250,000 noncitizens are registered to vote.[76] Secretary Mullin has called on each of these four states to collaborate with DHS to address these supposed instances of voter fraud.[77] President Trump has also singled out Minnesota for allegations of fraud, claiming that "[i]f the Elections in Minnesota weren't RIGGED, any Republican could win, but they were."[78]

133. Members of each of LWV, EPIC, and LULAC, including those who vote in the aforementioned jurisdictions and elsewhere, have been injured by the Voter Data Collection Policy

---

[75] Priscilla Alvarez et al., *Exclusive: DHS Plans to Launch Voter Fraud Investigation Surge Tuesday*, CNN (Aug. 31, 2026), https://perma.cc/98NQ-2JJG.

[76] DHS, *DHS Secretary Markwayne Mullin Sends Letters to Secretaries of State Warning About Non-Citizens on Voter Rolls* (July 17, 2026), https://perma.cc/T35R-VRAY.

[77] *Id.*

[78] Pres. Donald J. Trump (@realDonaldTrump), Truth Social (July 15, 2026), https://perma.cc/X4Y3-9UMB; *see also* Nick Corasaniti, *Why Is the Trump Administration Demanding Minnesota's Voter Rolls?*, N.Y. Times (Jan. 26, 2026), https://perma.cc/WS78-M4GJ.

because the policy deprives them of their privacy rights. Because these members have registered to vote and voted in the past, their sensitive personal information is contained in the files that DHS maintains pursuant to the Voter Data Collection Policy. These members reasonably fear and are emotionally distressed by the unauthorized disclosure and collection of their sensitive personal information. They further reasonably fear and are emotionally distressed by DHS's potential aggregation, misuse, and mishandling of their sensitive personal data. These injuries are caused by Defendants, who collected and are maintaining this information in violation of the Privacy Act and other legal constraints.

134. Members of each of LWV, EPIC, and LULAC also reasonably fear that DHS will inaccurately flag them as unlawful voters and create TECS records, resulting in consequences such as additional screening at the border, limiting their right to travel.

135. The collection and maintenance of the sensitive information of members of each of LWV, EPIC, and LULAC is causing, and will continue to cause, significant harm. Those harms include: the loss of members' statutory privacy rights; the misuse and repurposing of members' private data in unauthorized ways; the sharing, through unsecured means, of members' private data with unauthorized third parties with no lawful right to access it; members' unease and fears about the examination and transmission of their sensitive data by those who have accessed and will access it; the increased vulnerability of members' data to theft and security breaches; and the increased risk that members' data will be used to subject them to unwarranted investigations or impediments to their fundamental rights to vote or to travel.

Concrete Harms to Members

136. For example, one LWV member is a registered voter and a resident of Pennsylvania. This member believed that when she provided her information to Pennsylvania to register to vote, the information would be kept private. She has been a victim of identity theft in the past, which was

an extremely stressful and time-consuming experience, and she is worried that DHS's retention of her information would increase the risk of it happening again. The member understands that the more people have their hands on her personal information, the less secure it will be.

137. Another LWV member is a registered voter and a resident of Illinois. This member is a naturalized citizen and a former lawyer for the federal government. She is also concerned about DHS's efforts to collect her voter information. This member fears that DHS will use the voter registration information she has provided to the state to disqualify her from voting. She does not believe that DHS has any legitimate need for personal information like her address or telephone number. She specifically fears that DHS will obtain her political party information and will use that information to retaliate against her. As a former federal government lawyer, this member understands the Privacy Act. She is concerned that DHS is maintaining her information without following the correct legal procedures designed to protect her privacy. This member's personal information was compromised in the 2015 breach of Office of Personnel Management data. She understands, and is concerned about, the security risks associated with DHS's collection of her data.

138. A member of EPIC is a registered voter and a resident of Indiana. This member is an expert on the risks associated with the disclosure and aggregation of data beyond its intended purposes. She is concerned about the impact of DHS's efforts on her privacy. She considers the information she provided to register to vote to be private and did not consent to DHS collecting that information. She finds the sharing of her private information without her knowledge, expectation, or consent to be highly intrusive and offensive. This member takes steps to secure and protect personal information and to minimize the information she provides in all aspects of her life, including at the doctor's office. She is concerned about the data security implications of DHS's

efforts, especially given the speed at which DHS is collecting voter information and the agency's lack of experience in collecting and storing this information.

139. Another EPIC member is a registered voter and a resident of Texas. This member is a naturalized citizen. Previously, DHS's SAVE system falsely identified this member as a noncitizen based on out-of-date citizenship data. This member was removed from the voter rolls based on the faulty information in the SAVE system. He is concerned about DHS's history of mismanaging data. He fears that he will again be flagged as a noncitizen based on the voter information in DHS's files and will experience law enforcement consequences as a result. In addition, this member considered the information he provided when he registered to vote to be private and did not consent to DHS's acquisition of this information.

EPIC's Informational and Procedural Injuries

140. Plaintiff EPIC is suffering informational injuries as a result of the Voter Data Collection Policy.

141. EPIC's mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. Among other activities, EPIC monitors, analyzes, and educates the public about the collection, use, retention, and transfer of personal information by federal agencies. EPIC routinely submits comments on SORNs published in the Federal Register and other proposed agency actions related to information databases and mobilizes its members and partners to do the same.

142. For decades, EPIC has relied extensively on information that the Privacy Act and other statutes mandate agencies to disclose, including information in SORNs and notices of new or intended uses of information in systems of records. These documents are often the only publicly available records of how and why a federal entity is collecting personal information, what information is being collected, what burdens collection will impose, how that information may be

used and shared, how it will be stored and secured, and for how long it will be retained. EPIC depends on this public information to inform its research, advocacy, public education, and education of its members concerning the systems and databases used throughout the government. EPIC further relies on this information to craft targeted FOIA requests for agency records.

143. As explained above, Defendants failed to publish any SORN or notice of new or intended use in connection with the Voter Data Collection Policy. Because of Defendants' failure to disclose information required by statute, EPIC must expend resources on more burdensome methods of research and information gathering, including time-intensive FOIA requests, and likely litigation, to attempt to obtain timely access to relevant records, none of which is a substitute for the unique information Defendants have failed to create and publish as required by the Privacy Act.

144. Plaintiff EPIC is suffering a procedural injury as a result of the Voter Data Collection Policy.

145. EPIC frequently offers comments on proposed data collections during public comment periods. In its comments, EPIC leverages its experience and expertise to protect the public and its members with respect to issues affecting privacy rights.

146. As explained above, Defendants failed to engage in any period of public comment as required under federal law. In consequence, EPIC has also been denied an opportunity to comment on the Voter Data Collection Policy, to raise the privacy and security risks attendant to the federal government collecting and maintaining large volumes of personal information, and to offer potential solutions to safeguard sensitive personal information.

CLAIMS FOR RELIEF

COUNT I
Violation of the APA
Agency Action Contrary to Law and in Excess of Statutory Authority

147. Plaintiffs restate and reallege all paragraphs above as if fully set forth here.

148. Under the APA, courts must "hold unlawful and set aside agency action" that is "not in accordance with law" or "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(A), (C).

149. The Voter Data Collection Policy is "final agency action for which there is no other adequate remedy in a court" within the meaning of the APA. *Id.* § 704.

150. A federal agency "'literally has no power to act' . . . unless and until Congress authorizes it to do so by statute." *FEC v. Cruz*, 596 U.S. 289, 301 (2022) (quoting *La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986)).

151. No statute authorizes the Voter Data Collection Policy.

152. As DHS itself concedes, ICE and its component agency HSI "do[] not possess independent authority to administer or oversee elections" and "do[] not serve as the primary Federal agency enforcing election administration provisions under Title 52 of the U.S. Code."[79]

153. DHS lacks any statutory authority to engage in the mass collection and maintenance of voter files for the purpose of investigating systemic voter fraud, upholding election integrity, or protecting the voting process.

154. DHS further lacks any statutory authority to maintain SVRL data concerning many millions of Americans not under investigation for voter fraud or anything conceivably within DHS's jurisdiction.

155. DHS also lacks the statutory authority to maintain SVRL data for other purposes, including identifying deceased voters on state voter rolls.

---

[79] ICE, *Hot Topic: ICE's Role in Elections and at Polling Facilities*, at 7, *available at* https://perma.cc/Q6VE-W9UC (26-ICLI-00100 004).

156. The SVRLs and other records collected and maintained by Defendants as part of the Voter Data Collection Policy are created for election-related or commercial purposes and are unrelated to any individual's citizenship or immigration status.

157. The Voter Data Collection Policy is thus "not in accordance with law" and "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(A), (C).

COUNT II
Violation of the APA
Agency Action Contrary to the Privacy Act

158. Plaintiffs restate and reallege all paragraphs above as if fully set forth here.

159. Under the APA, courts must "hold unlawful and set aside agency action" that is "not in accordance with law." 5 U.S.C. § 706(2)(A).

160. The Privacy Act generally applies where an agency "maintains a system of records." *Id.* § 552a(e).

161. Each of the SVRLs and other records collected and maintained by Defendants as part of the Voter Data Collection Policy constitutes a "record" within the meaning of the Privacy Act because it is an "item, collection, or grouping of information about an individual that is maintained by [Defendants] . . . and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual." *Id.* § 552a(a)(4). The information collected and maintained pursuant to the Voter Data Collection Policy constitutes one or more "system[s] of records" within the meaning of the Privacy Act because they are a "group of any records under the control of [Defendants] from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *Id.* § 552a(a)(5).

162. Under the Voter Data Collection Policy, Defendants "maintain[]" these "record[s]" and "system[s] of records" because Defendants "maintain, collect, use, or disseminate" them. *Id.* § 552a(a)(3).

163. The Privacy Act prohibits agencies from disclosing records contained in a system of records except pursuant to certain exceptions. *Id.* § 552a(b). None of the exceptions for disclosure are met here.

164. The Privacy Act further prohibits agencies from maintaining 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." *Id.* § 552a(e)(7).

165. Registering to vote, voting, and affiliating with a political party are expressive and associational activities protected under the First Amendment. *See Buckley v. Am. Const. L. Found., Inc.*, 525 U.S. 182, 195 (1999); *Burdick v. Takushi*, 504 U.S. 428, 433 (1992); *Kusper v. Pontikes*, 414 U.S. 51, 57 (1973). The information collected and maintained under the Voter Data Collection Policy thus describes how individuals exercise rights guaranteed by the First Amendment.

166. No exception to the prohibition on maintaining records on First Amendment activity applies. No statute authorizes, much less expressly authorizes, the Voter Data Collection Policy. Few if any voters have authorized the federal government to collect and maintain their voter files. And the voting information collected and maintained under the Voter Data Collection Policy is not pertinent to or within the scope of an authorized law enforcement activity.

167. Furthermore, under the Privacy Act, agencies that maintain a system of records must also "maintain . . . only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. § 552a(e)(1).

168. Under the Voter Data Collection Policy, Defendants maintain voter information and other sensitive personal information for many of the approximately 174 million registered voters in the country. This information is not relevant or necessary to accomplish a purpose required to be accomplished by statute or executive order.

169. Finally, agencies must maintain records used "in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." *Id.* § 552a(e)(5).

170. Defendants have failed to maintain the voter files in their possession with sufficient accuracy to ensure fairness in making determinations about whether individuals have committed election fraud.

171. The Voter Data Collection Policy is therefore "not in accordance with" the substantive prohibitions imposed by the Privacy Act. *Id.* § 706(2)(A).

COUNT III
Violation of the APA
Agency Action Without Observance of Procedure Required by the Privacy Act

172. Plaintiffs restate and reallege all paragraphs above as if fully set forth here.

173. The APA requires courts to "hold unlawful and set aside" agency action that is "without observance of procedure required by law." 5 U.S.C. § 706(2)(D).

174. Under the Privacy Act, an agency establishing any system of records must publish in the Federal Register a SORN containing detailed information about the system. *Id.* § 552a(e)(4).

175. In addition, if a SORN identifies a new use of records, the agency must publish a separate notice in the Federal Register at least 30 days before publication of the SORN identifying "any new use or intended use of the information in the system, and provide an opportunity for interested persons" to comment. *Id.* § 552a(e)(11).

176. By adopting and implementing the Voter Data Collection Policy, Defendants have established and maintained a new or revised system of records.

177. Defendants have not, however, published a new or revised SORN.

178. Nor have Defendants disclosed any proposed new or intended use of records in a separate notice in the Federal Register. They likewise have failed to provide any opportunity for the public to comment on the proposed use of records.

179. Defendants have failed to either publish a system of records notice or follow the notice-and-comment procedures for new or intended uses of information.

180. The Voter Data Collection Policy is therefore "not in accordance with" and "without observance of [the] procedure required by" the Privacy Act. *Id.* § 706(2)(A), (D).

COUNT IV
Violation of the APA
Agency Action Without Observance of Procedure Required by the PRA

181. Plaintiffs restate and reallege all paragraphs above as if fully set forth here.

182. The APA requires courts to "hold unlawful and set aside" agency action that is "without observance of procedure required by law." 5 U.S.C. § 706(2)(D).

183. The PRA requires agencies to follow extensive procedures before engaging in any "collection of information." For example, the agency must conduct a review of the proposed collection of information, solicit and evaluate public comments, publish a second notice soliciting public comment, and obtain the approval of OMB. 44 U.S.C. §§ 3506–07.

184. "An agency shall not conduct or sponsor the collection of information unless" it has taken each of those steps "in advance of the adoption . . . of the collection of information." *Id.* § 3507(a).

185. The Voter Data Collection Policy constitutes a "collection of information" because it "obtain[s], caus[es] to be obtained, [and] solicit[s] . . . facts . . . calling for . . . answers to identical

questions posed to, or identical reporting . . . requirements imposed on, ten or more persons." *Id.* § 3502(3)(A)(i).

186. Defendants have not carried out the procedural steps required by the PRA. For example, they have not solicited a single round of public comments on the collection, much less allowed for the two required rounds.

187. The Voter Data Collection Policy is thus "not in accordance with" and "without observance of [the] procedure required by" the PRA. 5 U.S.C. § 706(2)(A), (D).

COUNT V
Violation of the APA
Arbitrary and Capricious Agency Action

188. Plaintiffs restate and reallege all paragraphs above as if fully set forth here.

189. The APA requires courts to "hold unlawful and set aside" agency action that is "arbitrary, capricious, [or] an abuse of discretion." 5 U.S.C. § 706(2)(A).

190. The Voter Data Collection Policy is arbitrary and capricious because, among other things, Defendants' investigation of up to 174 million Americans is overbroad; Defendants failed to consider the privacy and data security risks, ignored evidence of the rarity of noncitizen voting, and did not consider obvious alternatives to the policy; and Defendants implemented the policy in a secretive manner and provided states, voters, and other stakeholders with no information about how Defendants assemble, process, and use voter information.

PRAYER FOR RELIEF

Plaintiffs respectfully request that this Court:

a. Declare that the Voter Data Collection Policy, including Defendants' collection, maintenance, augmentation, and use of state voter registration files, is without statutory authority and violates the Privacy Act, the Paperwork Reduction Act, and the Administrative Procedure Act;

b. Hold unlawful, vacate, set aside, and permanently enjoin the Voter Data Collection Policy;

c. Order Defendants to delete and disgorge any voter information collected and maintained pursuant to the Voter Data Collection Policy;

d. Order Defendants not to use voter information collected and maintained pursuant to the Voter Data Collection Policy, including but not limited to using the information internally and sharing the information with DOJ;

e. Award Plaintiffs their costs, reasonable attorneys' fees, and other disbursements deemed appropriate; and

f. Grant such other relief as the Court deems necessary, just, and proper.

Dated October 15, 2026

Respectfully submitted,

/s/ Louis R. Katz

Louis R. Katz (D.C. Bar No. 90003861)
Briana M. Clark (D.C. Bar No. 1735505)
J.P. Cooney (D.C. Bar No. 494026)
Ronald A. Fein (D.C. Bar No. 90026641)
Brian D. Netter (D.C. Bar No. 979362)
Democracy Forward Foundation
P.O. Box 34553
Washington, DC 20043
Phone: (202) 448-9090
Fax: (202) 796-4426
lkatz@democracyforward.org
bclark@democracyforward.org
jpcooney@democracyforward.org
rfein@democracyforward.org
bnetter@democracyforward.org

John B. Hill (D.C. Bar No. 90044825)
Reuven Dashevsky (D.C. Bar No. 90046789)*
Haley Y. Florsheim (D.C. Bar No. 90041575)*
Nikhel S. Sus (D.C. Bar No. 1017937)
Citizens for Responsibility
and Ethics in Washington
P.O. Box 14596
Washington, DC 20044
(202) 408-5565
jhill@citizensforethics.org
rdashevsky@citizensforethics.org
hflorsheim@citizensforethics.org
nsus@citizensforethics.org

* *Pro hac vice* motion forthcoming

Counsel for Plaintiffs