IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue, NW
Washington, DC 20036,

Plaintiff,

v.

U.S. CITIZENSHIP AND IMMIGRATION SERVICES
5900 Capital Gateway Drive
Camp Springs, MD 20746
(Prince George's County),

JOSEPH B. EDLOW, in his official capacity as Director of the United States Citizenship and Immigration Services
5900 Capital Gateway Drive
Camp Springs, MD 20746
(Prince George's County),

U.S. SOCIAL SECURITY ADMINISTRATION
6401 Security Blvd.
Baltimore, MD 21235
(Baltimore County),

FRANK BISIGNANO, in his official capacity as Commissioner of the Social Security Administration
6401 Security Blvd.
Baltimore, MD 21235
(Baltimore County),

U.S. DEPARTMENT OF HOMELAND SECURITY
2707 Martin Luther King Jr Ave SE
Washington, DC 20528,

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Case No. _____

RETRIEVED FROM DEMOCRACYDOCKET.COM

MARKWAYNE MULLIN, in his official capacity as Secretary of the Department of Homeland Security,
2707 Martin Luther King Jr Ave SE
Washington, DC 20528,

U.S. DEPARTMENT OF STATE
2201 C St NW
Washington, DC 20451,

MARCO RUBIO, in his official capacity as Secretary of the Department of State
2201 C St NW
Washington, DC 20451,

Defendants.

RETRIEVED FROM DEMOCRACYDOCKET.COM

INTRODUCTION

1. Multiple statutes restrict federal agencies from sharing and disseminating Americans' sensitive personal information. And the Constitution gives states—not the Executive Branch—authority over determining voter eligibility and federal election procedures. Yet, in its attempt to seize control over elections, the Trump Administration has brushed aside these laws and constitutional limits by ordering the mass centralization and sharing of Americans' data for ultimate use in determining voter eligibility.

2. This suit challenges illegal agency action to implement Section 2(a) of the President's Executive Order No. 14399, *Ensuring Citizenship Verification and Integrity in Federal Elections*, 91 Fed. Reg. 17125 (March 31, 2026) (the "2026 Elections EO" or "EO").

3. Section 2(a) directs federal agencies "to compile and transmit to the chief election official of each State a list of individuals confirmed to be United States citizens who will be above the age of 18 at the time of an upcoming Federal election and who maintain a residence in the subject State (State Citizenship Lists) . . . no fewer than 60 days before each regularly scheduled Federal election." *Id.* Indeed, DHS has committed it will—and "must"—complete and transmit these lists no later than **September 4, 2026**.

RETRIEVED FROM DEMOCRACYDOCKET.COM

4. In scrambling to implement this directive before the November election, the Department of Homeland Security ("DHS"), Social Security Administration ("SSA"), and Department of State ("DOS") finalized a policy to disclose hundreds of millions of Americans' sensitive personal information to state election officials through a new online "portal" (the "State Citizenship Lists Portal" or "Portal"). *See* Memorandum from Joseph B. Edlow, Director, U.S. Citizenship and Immigration Services ("USCIS") for the DHS Secretary, Executive Order 14399 Implementation 2–3 (June 8, 2026) ("Implementation Memo") (attached as Ex. A). Separately,

DHS will use the information compiled in this Portal to create its own "consolidated list of United States citizens and residents of the applicable State to provide to state election officials no fewer than 60 days before each regularly scheduled federal election." *Id.* at 3. DHS consummated this policy in a memorandum approved by the DHS Secretary on June 8. *Id.* at 5.

5. Defendants' actions are flagrantly unlawful. No statute authorizes Defendants to share and centralize vast volumes of Americans' sensitive personal data across government agencies to create and disclose the "State Citizenship Lists." And in doing so, Defendants are running roughshod over critical safeguards of the Social Security Act, the Privacy Act, and the Administrative Procedure Act ("APA"), and the constitutional separation of powers.

RETRIEVED FROM DEMOCRACYDOCKET.COM

6. Defendants' actions imperil millions of Americans' privacy and voting rights. Defendants are creating the State Citizenship Lists by repurposing data the government admits is unreliable, outdated, and incomplete. That is especially true for U.S. citizens who were born abroad, are over 45years old, have changed names, or move frequently. DHS is aggressively pushing state election officials to use this admittedly unreliable data to purge their voter rolls of purported non-citizens—under threat of "fines," "penalties," and even "prison time." Nick Corasaniti & Dustin Volz, *Markwayne Mullin reiterates Trump's false claims about voting security*, N.Y. Times (July 17, 2026), https://tinyurl.com/mpe6wu2h.

7. Defendants' list-making scheme is well underway. A DHS website announces the "State Citizenship Lists Portal" is "Coming Soon." *See* USCIS, State Citizenship Lists, https://perma.cc/7N5H-WRS7. The Implementation Memo makes clear DHS "must" launch the Portal "within the timeframe directed by EO 14399," Ex. A at 4—*i.e.*, by September 4, 2026. Defendants have indicated in recent court filings that they will meet that deadline. *See* Application for a Stay at 27, *Trump v. California*, No. 26A124, 2026 WL 2170485 (U.S. July 27, 2026).

8. Plaintiff, a national privacy rights organization whose members and mission are directly harmed by Defendants' illegal actions, respectfully requests that this Court intervene.

PARTIES

9. **Plaintiff Electronic Privacy Information Center ("EPIC")** is a nonprofit organization headquartered in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC is devoted to securing the right to privacy in the digital age, and central to this mission is oversight and analysis of government activities that affect individual privacy. Among its activities, EPIC engages in advocacy, research, and public education about the collection, use, retention, and disclosure of personal information by federal agencies, including large-scale databases and mass surveillance programs.

10. EPIC is a membership organization. A 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. EPIC has many members across 31 states, including Maryland.

RETRIEVED FROM DEMOCRACYDOCKET.COM

11. **Defendant U.S. Citizenship and Immigration Services ("USCIS")** is an agency within the meaning of the Privacy Act and the APA, and is headquartered in Camp Springs, Maryland.

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

13. **Defendant U.S. Social Security Administration** is an agency within the meaning of the Privacy Act and the APA, and is headquartered in Baltimore County, Maryland.

14. **Defendant Frank Bisignano** is the Commissioner of SSA and is sued in his official capacity.

15. **Defendant U.S. Department of State** is an agency within the meaning of the Privacy Act and the APA, and is headquartered in Washington, DC.

16. **Defendant Marco Rubio** is the Secretary of DOS and is sued in his official capacity.

17. **Defendant U.S. Department of Homeland Security** is an agency within the meaning of the Privacy Act and the APA, and is headquartered in Washington, DC.

18. **Defendant Markwayne Mullin** is the Secretary of DHS and is sued in his official capacity.

RETRIEVED FROM DEMOCRACYDOCKET.COM

JURISDICTION AND VENUE

19. 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 APA, 5 U.S.C. §§ 701–706.

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

STATUTORY BACKGROUND

21. The creation and dissemination of the State Citizenship Lists run afoul of two key federal statutes that create substantive and procedural protections regarding the government's handling of Americans' sensitive personal data: the Privacy Act and the Social Security Act.

Restrictions on disclosure of Social Security information

22. As SSA has long recognized, "the SSN [(Social Security Number)] is one of the most sensitive pieces of personal information in [its] records" because "of its use as a unique identifier," and it "is the key to identifying and retrieving most of the highly personal and sensitive

information [SSA] maintain[s] about individuals." SSA, Programs Operations Manual System ("POMS") GN 03325.002, *Disclosure and Verification of Social Security Numbers (SSN) Without Consent* (2023), https://perma.cc/PE44-2QBK ("SSA Disclosure Policy"). Due to the special sensitivity of SSNs and other SSA records, various statutes, regulations, and agency policies restrict the data's disclosure, verification, and use.

23. First, the Social Security Act prohibits SSA from "disclosure" of "any file, record, report, or other paper, or any information" except as the SSA Commissioner "may by regulations prescribe" or "as otherwise provided by Federal law." 42 U.S.C. § 1306(a)(1); *see also* 20 C.F.R. § 401.135.

24. Second, the Social Security Act prohibits *any* federal official (not just SSA personnel) from disclosing "[s]ocial security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law enacted on or after October 1, 1990." 42 U.S.C. § 405(c)(2)(C)(viii)(I).

RETRIEVED FROM DEMOCRACYDOCKET.COM

25. Third, SSA's policy manual provides that the agency will disclose or "verify SSNs, and SSN information" only "under limited circumstances as allowed or required by Federal laws," where SSA has express "legal authority and where [it is] able to identify the true number holder." SSA Disclosure Policy, *supra*. For SSA to verify SSNs pursuant to a federal statute, "the statute must *specifically mandate* that SSA disclose SSNs." *Id.* (emphasis added).

26. Fourth, SSA's policy manual recognizes that SSA does "not have the legal authority to disclose information about U.S. citizens to DHS," and that "[i]f DHS requests information and we determine the information pertains to both U.S. citizens and aliens, only information about the aliens can be disclosed." *Id.*; *accord* SSA, POMS GN 03313.095 *Disclosure to the Dep't of Homeland Security (DHS)* (2025), https://perma.cc/NZR7-MVB7.

The Privacy Act restricts disclosure and consolidation of Americans' personal information

27. Congress enacted the Privacy Act of 1974 to prevent the government from creating "formal or de facto national data banks" or "centralized Federal information systems" that would consolidate sensitive personal data of Americans stored at separate agencies in ways that could endanger our fundamental rights. Staff of S. & H. Comms. on Gov't Operations, 94th Cong., *Legislative History of the Privacy Act of 1974: Source Book on Privacy* 168, 217, 884 (Joint Comm. Print 1976), https://perma.cc/9W9F-R5ZL. Congress sought to protect against such "interagency computer data banks" in order to make it "legally impossible for the Federal Government in the future to put together anything resembling a '1984' personal dossier on a citizen," and to ensure "proper regard for privacy of the individual, confidentiality of data, and security of the system." *Id.* at 217, 884.

RETRIEVED FROM DEMOCRACYDOCKET.COM

28. To that end, the Privacy Act establishes a series of substantive and procedural "safeguards for an individual against an invasion of personal privacy by requiring Federal agencies" to "collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose," and ensuring "that adequate safeguards are provided to prevent misuses of such information." Privacy Act of 1974 § 2(b)(4), 88 Stat. 1896 (codified at 5 U.S.C. § 552a & note (Congressional Findings and Statement of Purpose)).

29. As pertinent here, the Privacy Act makes it "unlawful for an agency to disclose a record to another agency" or to any other entity "without the written consent of the person to whom the record pertains," subject to "certain exceptions." *FAA v. Cooper*, 566 U.S. 284, 289 n.2 (2012) (citing 5 U.S.C. § 552a(b)). One such exception is disclosure under a properly noticed "routine use," 5 U.S.C. § 552a(b)(3), defined as a use "for a purpose which is compatible with the purpose for which [a record] was collected," *id.* § 552a(a)(7).

30. The Act requires each agency that maintains a system of records to take certain steps to ensure the records it "maintains" on individuals are accurate, relevant, up-to-date, and secure, *see* 5 U.S.C. §§ 552a(e)(5), (6), (10), in order to prevent "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained," *id.* § 552(e)(10). The Act defines "maintain" to include "maintain, collect, use, or disseminate." *Id.* § 552a(a)(3).

31. The Act also imposes strict notice-and-comment requirements. When agencies "establish[] or revis[e]" any "system of records" containing retrievable information about individuals, they must "publish in the Federal Register … a notice,"—called a System of Records Notice ("SORN")—disclosing the system's contents, functions, uses, and procedures for individuals to access and correct records about themselves. *Id.* § 552a(e)(4).

32. Agencies must publish a SORN at least 30 days *before* "any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments." *Id.* § 552a(e)(11). Agencies must also provide notice to Congress. *Id.* § 552a(r).

33. Privacy Act guidelines issued by the Office of Management and Budget ("OMB"), per a statutory delegation, *see* 5 U.S.C. § 552a(v)(1), confirm that the Act requires a meaningful opportunity for notice and comment *before* Americans' personal data is used in substantially new ways. *See* Privacy Act Guidelines, 40 Fed. Reg. 28949, 28966 (July 9, 1975), https://perma.cc/776J-4L46; Off. of Mgmt. & Budget, Exec. Off. of the President, OMB Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* 7, 12 (2016), https://perma.cc/N9QK-SDLE ("OMB Circular No. A-108").

RETRIEVED FROM DEMOCRACYDOCKET.COM

34. Examples of "significant changes" to a system of record that require publication of a modified SORN include a "substantial increase in the number, type, or category of individuals about whom records are maintained in the system"; a "change that expands the types or categories of records maintained in the system"; a "change that modifies the purpose(s) for which the information in the system of records is maintained"; a "change that modifies the scope of the system," such as "combining of two or more existing systems of records"; and a "new routine use or significant change to an existing routine use that has the effect of expanding the availability of the information in the system." OMB Circular No. A-108 at 5–6.

FACTUAL BACKGROUND

RETRIEVED FROM DEMOCRACYDOCKET.COM

The Administration's ongoing attempt to federalize election administration

35. The Constitution assigns to the States—not the President—authority over elections. It vests the States with the authority to determine voter eligibility and (shared with Congress) the power to regulate federal election procedures. U.S. Const. art. I, § 2, cl. 1; *id.* amend. XVII; *id.* art. I, § 4, cl. 1.

36. Despite this constitutional reality, in his second term, President Trump has sought to "take over" and "nationalize" elections. ABC 7 Chicago, *Trump urges Republicans to 'take over' and 'nationalize' voting* (YouTube, Feb. 3, 2026), https://tinyurl.com/4nfv2tdt.

37. The President wrongly claims that "the States are merely an 'agent' [sic] for the Federal Government in counting and tabulating the votes. They must do what the Federal Government, as represented by the President of the United States, tells them, FOR THE GOOD OF OUR COUNTRY, to do." Donald J. Trump (@realDonaldTrump), Truth Social (Aug. 18, 2025, at 7:17 AM ET), https://tinyurl.com/2ha9cmfv [https://perma.cc/9E2W-8ZSQ].

38. The President is particularly fixated on baseless claims about widespread voting by non-citizens. *See, e.g.*, Donald J. Trump (@realDonaldTrump), Truth Social (Aug. 18, 2025, at 4:48 PM ET), https://tinyurl.com/57uuadnw [https://perma.cc/USN6-WVFK].

39. As a result, the President has pursued countless investigations, signed two executive orders, and championed multiple (failed) bills all aimed at federalizing election administration, despite lacking any authority to make or amend laws governing elections.

40. Consolidating and disclosing millions of Americans' sensitive personal information across federal and state agencies, for purposes of enabling mass "voter verification" checks, is central to the Administration's attempt to nationalize election administration.

RETRIEVED FROM DEMOCRACYDOCKET.COM

The 2025 Elections EO and the Modified SAVE system

41. On March 25, 2025, President Trump signed Executive Order No. 14248, *Preserving and Protecting the Integrity of American Elections*, 90 Fed. Reg. 14005 (Mar. 25, 2025) (the "2025 Elections EO").

42. The 2025 Elections EO instructs DHS to "share database information with States upon request" under "8 U.S.C. 1373(c)" for voter list maintenance purposes, and directs DHS to compare voter records with "Federal immigration databases." 2025 Elections EO §§ 1, 2(b)(iii). The EO also directs SSA to make its databases available "to all State and local election officials" for "verifying" voter eligibility. *Id.* § 3(a).

43. To implement these directives, DHS and SSA haphazardly made major changes to USCIS's Systematic Alien Verification for Entitlements ("SAVE") system in 2025 (the "Modified SAVE system"). *See* Notice of Modified System of Records, 90 Fed. Reg. 48948, 48949–51 (Oct. 31, 2025).

44. Internal agency records reveal that DHS knew the SAVE modifications were "not in compliance with" the Privacy Act and that, due to "shortfalls in data accuracy," the modified system could not reliably confirm citizenship for citizens born outside of the United States. DHS, *Privacy Threshold Analysis for the SAVE Program* 17, 34, 38–39 (approved July 17, 2025), https://perma.cc/9AXY-WCLU; *see also* DHS, DHS Ref. No. DHS/USCIS/PIA-006(d), *Privacy Impact Assessment for the Systematic Alien Verification for Entitlements "SAVE" Program* 19 (Oct. 31, 2025), https://perma.cc/G92U-LYPM (warning SAVE "may share inaccurate information with registered agencies" and "may produce inaccurate results").

45. Disregarding these known problems, DHS has pushed states to bulk upload their entire statewide voter lists into the Modified SAVE system for mass citizenship checks. Early results have shown that SAVE's mistakes are widespread, with error rates as high as 81% in some localities. *See* Jen Fifield & Zach Despart, *"Not Ready for Prime Time." A Federal Tool to Check Voter Citizenship Keeps Making Mistakes*, ProPublica & Tex. Trib. (Feb. 13, 2026), https://perma.cc/PR4Q-67NR; Judd Legum & Rebecca Crosby, *The Federal Database That Could Upend the Midterm Elections*, Mother Jones (Apr. 9, 2026), https://perma.cc/8YXC-WU7U.

RETRIEVED FROM DEMOCRACYDOCKET.COM

46. On June 22, 2026, the U.S. District Court for the District of Columbia held unlawful, vacated, and set aside DHS's and SSA's 2025 modifications to the SAVE system. *See League of Women Voters v. DHS*, No. 25-cv-3501-SLS, 2026 WL 1784297, at *2 (D.D.C. June 22, 2026), *appeal docketed*, No. 26-5243 (D.C. Cir. June 29, 2026) ("*LWV*").

47. The *LWV* court held that the SAVE modifications and the inter-agency data disclosures they enable violated the Social Security Act, *id.* *20; violated the Privacy Act, *id.* at *23–28; were arbitrary and capricious under the APA, *id.* at *28–30; and lacked statutory authorization, *see id.* at *30–33. The court explicitly rejected DHS's and SSA's position (also at

issue in this case, *see infra* ¶¶ 67, 136, 146) that 8 U.S.C. § 1373 authorizes the agencies to freely disclose citizen status information to each other and to states notwithstanding the pre-existing statutory restrictions on such inter-agency data sharing and consolidation. *Id.* at *32–33.

The 2026 Elections EO and State Citizenship List process

48. After failing to secure enactment of his desired changes to election administration from Congress,[1] the President signed a second executive order on elections on March 31, 2026. *See* 2026 Elections EO, 91 Fed. Reg. 17125. This suit challenges Defendants' actions to implement Section 2(a) of the EO.

49. **Section 2** creates a new federal program designed to exert federal control over States' voter rolls and voter eligibility. Specifically, Section 2(a) directs the Secretary of DHS, through the Director of USCIS and in coordination with the SSA Commissioner, to develop for each state "a list of individuals confirmed to be United States citizens who will be above the age of 18 at the time of an upcoming Federal election and who maintain a residence in the subject State," deemed the "State Citizenship List." 2026 Elections EO § 2(a). Though residence for purposes of voter eligibility is a question of state law, the 2026 Elections EO anticipates the Secretary will make residency determinations when compiling the list. *Id.*

RETRIEVED FROM DEMOCRACYDOCKET.COM

50. The State Citizenship Lists are to be compiled from "citizenship and naturalization records, SSA records, SAVE data, and other relevant Federal databases." *Id.*

[1] The President has pushed Congress to enact multiple bills authorizing expansive cross-agency data sharing for purposes of state "voter verification" queries. *See* SAVE America Act, H.R. 7296, 119th Cong. § 2(f) (2026) (authorizing, among other provisions, use of SAVE for bulk voter verification and directing that all agency heads "shall share information with each other" to enable voter verification inquiries); *accord* SAVE Act, H.R. 22, 119th Cong., § 2(f) (2025); SAVE Act, H.R. 8281, 118th Cong., § 2(f) (2024). None of these bills have passed the Senate.

51. The State Citizenship Lists are to be sent to States' chief elections officials "no fewer than 60 days before each regularly scheduled Federal election, or promptly upon request by a State in connection with any special Federal election." *Id.* The deadline for the State Citizenship Lists to be sent for the November 2026 elections is **September 4, 2026**.

52. A related provision of the 2026 Elections EO sets a 90-day deadline for the DHS Secretary to "establish the infrastructure necessary to compile, maintain, and transmit the State Citizenship List" and requires the SSA Commissioner to "provide all necessary citizenship and identity data to the Secretary of Homeland Security" to support the creation of the list. *Id.* § 4(c).

53. Section 2(a) further directs the DHS Secretary to "establish procedures to (i) allow individuals to access their individual records as well as to update or correct them in advance of elections; and (ii) enable States to routinely supplement and provide suggested modifications or amendments to the [list]." *Id.* § 2(a). The EO does not require the DHS Secretary to accept suggested modifications and amendments; rather, the final list is within exclusive federal control. *See id.*

RETRIEVED FROM DEMOCRACYDOCKET.COM

54. Section 2 pairs the provision of the State Citizenship Lists to state elections officials with an explicit threat of criminal prosecution: It directs the Attorney General to prioritize the investigation and prosecution of "State and local officials" or others "who issue Federal ballots to individuals not eligible to vote in a Federal election." *Id.* § 2(b); *see also id.* § 5. Section 2(b) defines "eligible to vote in a Federal election" to require, among other things, that the person is "18 years of age or older by the date of the upcoming election[.]" *Id.* § 2(b).

55. Thus under Section 2(b), "State and local officials or any others involved in the administration of Federal elections who issue Federal ballots" to voters not on the federal State

Citizenship Lists face an acute risk of criminal prosecution simply for doing their jobs in compliance with state and federal law. *See id.*

56. On June 8, 2026, DHS Secretary Mullin signed and approved USCIS's implementation memo for Section 2(a) of the 2026 Elections EO. *See* Ex. A at 5; *infra* ¶¶ 61–77.

57. **Section 3** of the 2026 Elections EO interposes the U.S. Postal Service ("USPS") into States' administration of voting. EO § 3(b). Section 3 mandates, among other things, that each state notify USPS whether it intends to submit "a list of voters eligible to vote in a Federal election" via mail. *Id.* § 3(b)(ii). USPS must then create and provide each state with a list of people enrolled with USPS for mail-in or absentee ballots, named the "Mail-In and Absentee Participation List." *Id.* § 3(b)(iv). USPS must establish procedures for each state to supplement and suggest amendments to the list in advance of an election. *Id.* § 3(b)(v). Section 3 prohibits USPS from transmitting a mail ballot from any voter not included on the Mail-In and Absentee Participation List. *Id.* § 3(b)(iii). Section 3 concludes with explicit threats of criminal prosecution for states, their elections officials, and voters who make "unlawful use of the mail in connection with elections." *Id.* § 3(a); *see also id.* §§ 3(c), 5.

RETRIEVED FROM DEMOCRACYDOCKET.COM

58. On June 2, 2026, USPS published a notice of proposed rulemaking consistent with section 3. Ballot Mail for Federal Elections, 91 Fed. Reg. 32915 (proposed June 2, 2026) (to be codified at 39 C.F.R. pt. 111). USPS published the final rule on August 26, 2026. Ballot Mail for Federal Elections, 91 Fed. Reg. 54966 (Aug. 26, 2026).

59. **Section 4** effectuates Section 2, specifying that "[t]he Secretary of Homeland Security, the Commissioner of SSA, and the Postmaster General shall coordinate with the Secretary of Commerce" on "all relevant aspects of the implementation." *Id.* § 4(a). Section 4 also provides that the Secretary of Homeland Security shall "establish the infrastructure necessary to

compile, maintain, and transmit the State Citizenship List described in section 2(a)" and "designate a point of contact within DHS to receive and process requests from individuals and State election officials regarding the relevant State Citizenship List." *Id.* § 4(c) Finally, Section 4 directs the Commissioner of SSA to provide "all necessary citizenship and identity data to the Secretary of Homeland Security" in support of the requirement to "compile, maintain, and transmit" the State Citizenship Lists. *Id.*

60. **Section 5** threatens States and localities with federal funding cuts for any "noncompliance with Federal law" and reiterates threats of investigations and criminal prosecutions for State and local entities and elections officials. *Id.* § 5.

DHS's June 8 Implementation Memo

61. On June 8, DHS Secretary Mullin signed a memorandum "approv[ing]" a policy and "course of action" for "implementing Section 2(a)" of the EO. *See* Ex. A at 1, 5. This Implementation Memo rescinded and superseded a previous plan, explaining that the updated memo more accurately "reflect[s] the current policy of the Administration" with respect to the implementation of the EO. *Id.* at 1. The Implementation Memo explains that, given the scope and significance of the decision, and the required "coordination" with "SSA, DOS, and USPS," Secretary-level approval was "required to authorize" it. *Id.* at 4.

RETRIEVED FROM DEMOCRACYDOCKET.COM

62. The Implementation Memo approves a two-part process to implement Section 2(a).

63. **First**, DHS commits to creating a "federated portal" through which "state election officials … will be able to download separate outputs from USCIS, SSA, and DOS." *Id.* at 2–3. Implicit within this are SSA's and DOS's decisions to disclose confidential information for the Portal. "The downloaded files will provide citizenship related data elements, such as name, date of birth, and relevant agency identifiers." *Id.* at 2. For SSA, the "relevant agency identifier[]"

would be an SSN. *See id.*; SSA Disclosure Policy, *supra* (SSN is "the key to identifying and retrieving most of the highly personal and sensitive information we maintain about individuals").

64. Although the memo acknowledges the EO requires a "citizen facing portal" "through which individual citizens can view their own records and submit corrections," it states that USCIS "does not believe it is feasible to deliver a production ready citizen facing portal on or about June 30, 2026." *Id.* at 3. DHS thus decided to defer establishing this "transparency and redress function" for citizens until "later in 2026," *after* making the Portal available to the states. *Id.* "By focusing first on a federated, state-facing portal and by planning citizenship-facing transparency as a *follow-on* enhancement," the memo explains, "DHS can meet the EO's near term requirements while positioning itself for further improvements once legal and privacy work is complete." *Id.* at 4 (emphasis added).

RETRIEVED FROM DEMOCRACYDOCKET.COM

65. The Implementation Memo commits to "delivering" the Portal "enabling States to access citizenship related data" "on or about June 30, 2026," and not later than the deadline "directed by EO 14399"—60 days before the November election (September 4, 2026). *Id.* at 3–4.

66. **Second**, in addition to creating the Portal, the memo states that "DHS will continue to work to generate from the information contained in this portal a consolidated list of United States citizens and residents of the applicable State to provide to state election officials no fewer than 60 days before each regularly scheduled Federal election." *Id.* at 5.

67. The Implementation Memo claims that the expansive inter-agency data disclosure it requires is authorized by 8 U.S.C. § 1373, *see* Ex. A at 2—the same statute that DHS and SSA claimed authorized their disclosures through the Modified SAVE system. *See LWV*, 2026 WL 1784297, at *30-33 (rejecting that claim).

68. The Implementation Memo also states that Defendants' "privacy offices and counsel" are already "coordinating to ensure that . . . States' use, retention, and redisclosure of the information [contained in the State Citizenship Lists] are constrained through appropriate agreements and terms of service." Ex. A at 3.

69. No operative SORN published by DHS, SSA, or DOS authorizes the expansive new inter-agency information-sharing or consolidation approved in the Implementation Memo. Nor does the Implementation Memo describe any plans for DHS, SSA, or DOS to issue modified SORNs or conduct notice-and-comment in accordance with the Privacy Act—either for agency records they disclose to states through the new Portal, or for the records DHS compiles to create consolidated lists of citizens and residents to provide to state election officials.

70. To the contrary, the Implementation Memo's timelines and "phased delivery" approach are facially inconsistent with the Privacy Act's notice-and-comment requirements for new or modified systems of records.

71. The memo says the Portal would go live on June 30—just 22 days after the memo was issued, and in violation of the Privacy Act's required 30 days' advance notice (via a SORN) and meaningful consideration of any public comments. *See* 5 U.S.C. § 552a(e)(4), (11).

72. The memo also defers creation of the "transparency and redress function" for citizens to "view their own records and submit corrections" until an unspecified date "later in 2026." Ex. A at 3. This conflicts with the Privacy Act's requirement that agencies establish and publicly disclose procedures for individuals to access and correct their records at least 30 days *before* establishing a new or modified system of records. *See* 5 U.S.C. § 552a(e)(4)(H).

73. On June 25, 2026, a court enjoined DHS from implementing Sections 2 and 3 of the Executive Order as to 23 states and the District of Columbia, preventing DHS from meeting

RETRIEVED FROM DEMOCRACYDOCKET.COM

the June 30 target date for launching the Portal. *See California v. Trump*, No. 26-cv-11581, 2026 WL 1826490, at *17–18 (D. Mass. June 25, 2026). However, on August 24, the Supreme Court stayed the injunction on threshold grounds (standing and ripeness) without reaching the merits. *See Trump v. California*, No. 26A124, 2026 WL 2473573 (U.S. Aug. 24, 2026) ("The Court's disposition of this application does not mean that any measure taken by the Government to implement the Order will necessarily be lawful."). Following that ruling, Defendants have, on information and belief, resumed implementing the plan outlined in the Implementation Memo.

74. Indeed, the Implementation Memo insists "USCIS *must* establish the infrastructure to compile, maintain, and transmit State Citizenship Lists, and designate a DHS point of contact for those lists, within the timeframe directed by EO 14399," Ex. A at 4 (emphasis added)—*i.e.*, by September 4, 2026.

RETRIEVED FROM DEMOCRACYDOCKET.COM

75. Defendants' representations in court filings confirm they will implement Section 2 of the EO, including distributing the State Citizenship Lists by September 4 for use in the November 2026 election. *See* Application for a Stay at 27, *Trump v. California*, 2026 WL 2473573 (No. 26A124) (arguing that "[a]bsent a stay" of the injunction of Section 2(a) and other provisions of the EO, "the government will be unable to obtain appellate relief from an order that bars implementation of a presidential policy that seeks to ensure voter integrity in the upcoming November 2026 election").

76. Secretary Mullin has indicated that state election officials who refuse to use and effectuate the State Citizenship Lists ahead of the November election will face investigation, fines, and even imprisonment. *See* Nick Corasaniti & Dustin Volz, *supra*.

77. DHS has secured a domain for the State Citizenship Lists Portal: https://origin-statecitizenshiplists.uscis.dhs.gov/. A banner on that page, depicted below, reads: "Coming Soon" "State Citizenship Lists Portal."

Litigation challenging the 2026 Elections EO

78. Multiple lawsuits have directly challenged the 2026 Elections EO, including: *California v. Trump*, No. 26-cv-11581, 2026 WL 1826490 (D. Mass. June 25, 2026); *California v. USPS*, No. 1:26-cv-13917, 2026 WL 2539946 (D. Mass. Aug. 27, 2026); *League of Women Voters of Mass. v. Trump*, 1:26-cv-11549, 2026 WL 2539946 (D. Mass. Aug. 27, 2026); *DSCC v. Trump*, No. 26-CV-01114, 2026 WL 1487833 (D.D.C. May 28, 2026) (three consolidated cases).

79. However, as it stands at the time of this filing, there is no court order in effect that addresses the legality of the Defendants' actions to implement Section 2 of the EO, which is the focus of this suit.

RETRIEVED FROM DEMOCRACYDOCKET.COM

The government has repeatedly admitted the State Citizenship Lists' underlying data sources are incomplete, error-prone, and unreliable

80. The State Citizenship Lists must be compiled from "citizenship and naturalization records, SSA records, SAVE data, and other relevant Federal databases." 2026 Elections EO § 2(a). But none of these data sources can reliably verify citizenship, let alone state of residence, for purposes of determining voter eligibility.

81. SSA has repeatedly recognized that its citizenship data is incomplete and unfit for verifying citizenship. SSA's citizenship data is especially unreliable for citizens born outside of

the United States because it reflects a person's citizenship status when they *applied* for an SSN and does not automatically update if the person later becomes a citizen. *See* Letter from Nancy Morales Gonzalez, Assoc. Gen. Couns., SSA, to Jon Sherman, Litig. Dir. & Senior Couns., Fair Elections Ctr., Re: Application for Records and Testimony of a Social Security Administration (SSA) Employee in a Federal Civil Case 2 (July 13, 2023), https://perma.cc/KS2N-U2US. In addition, SSA's citizenship data for individuals older than 45 is incomplete because "SSA did not begin to consistently maintain citizenship information until 1981." *Id.*

82. SSA has accordingly warned against repurposing its citizenship data for other uses, explaining that while "citizenship information is accurate for SSA's program purposes, if used later for other purposes, it may not be current" because "SSA is not the custodian of U.S. citizenship records." *Id.*

83. DHS has likewise acknowledged data gaps in its SAVE system, which relies heavily on SSA's citizenship data. *See supra* ¶ 44. And it has confirmed that SAVE's data gaps are especially likely to impact citizens born outside of the United States, stating in recent guidance that "if an individual with acquired citizenship has not received a Certificate of Citizenship from USCIS (e.g., some foreign-born children of U.S. citizens) or is not designated as a U.S. citizen in SSA records, SAVE may not be able to confirm that individual's U.S. citizenship." USCIS, *Voter Registration and Voter List Maintenance Fact Sheet* (Aug. 27, 2025), https://perma.cc/Q5F7-YBCA.

84. Further, citizens who have moved regularly and changed their names are particularly vulnerable to being misidentified in the State Citizenship Lists. *See*, *e.g.*, Defendants' Statement of Undisputed Facts at 3 ¶ 19, *League of Women Voters v. Trump*, No. 26-cv-11581 (D.

RETRIEVED FROM DEMOCRACYDOCKET.COM

Mass. May 7, 2026), ECF No. 155 ("Undisputed that a significant number of people move between States each year, including eligible voters who move during the 60 days before an election.").

85. Although the State Citizenship Lists must include all citizens "who maintain a residence in the subject State," Ex. A at 1, there is no federal database that maintains accurate, up-to-date residency information for every household (let alone citizen) in the United States. *See e.g., Husted v. A. Philip Randolph Inst.*, 584 U.S. 756, 765 (2018) (describing unreliability of the USPS's National Change of Address Database because "according to the Postal Service '[a]s many as 40 percent of people who move do not inform the Postal Service'" (alteration in original)); Treasury Inspector Gen. for Tax Admin., Reference No. 2019-40-074, *Additional Actions Are Needed to Further Reduce Undeliverable Mail* (Sept. 11, 2019), https://perma.cc/5R66-8HSP (describing inaccuracy of IRS's address data).

RETRIEVED FROM DEMOCRACYDOCKET.COM

INJURIES TO PLAINTIFFS

86. Plaintiff EPIC and its members are suffering, and will continue to suffer, injuries as a result of Defendants unlawfully compiling, misusing, and sharing their personal information.

Injuries to EPIC's members

87. EPIC's members have suffered privacy and reputational injuries. They did not consent to the aggregation, misappropriation, or disclosure of their personally identifying information by Defendants. They are injured by Defendants' unauthorized collection, consolidation, and disclosure of this highly sensitive personal data—including their citizenship statuses, dates of birth, SSA data, DOS data, and other information. Neither the 2026 Elections EO nor the Implementation Memo permit them to opt out of having their sensitive personal information accessed, compiled, and disclosed for purposes unrelated to the reasons it was originally collected.

88. EPIC members have joined EPIC because they are concerned about personal privacy, safety, and security.

89. EPIC members whose personal data is being collected, consolidated, added to a list, shared, and misused by Defendants have a right to keep this sensitive data private. The unauthorized disclosure of such data would be highly offensive to a reasonable person.

90. Moreover, the improper disclosure of EPIC members' sensitive personal information, including in a portal made available to state governments and subject to unknown access restrictions, materially heightens the risk that the EPIC members' data will be misused or otherwise obtained by hackers or other unauthorized third parties. Upon information and belief, such unauthorized third parties frequently test government databases for vulnerabilities and seek to obtain government-held personal data to use for fraud, theft, and similar purposes.

RETRIEVED FROM DEMOCRACYDOCKET.COM

91. With respect to SSA data, EPIC members interacted in confidence with SSA for specific, narrow purposes. They reasonably expected that the privacy of their sensitive SSA information would be protected by the explicit guarantees of the Privacy Act and the Social Security Act. They also reasonably expected protection based on longstanding SSA policy recognizing that "the SSN is one of the most sensitive pieces of personal information in our records," assuring that SSA will "only verify SSNs without consent" in "narrow circumstances in which we have legal authority," and explicitly affirming that SSA "does not have the legal authority to disclose information about U.S. citizens to DHS." SSA Disclosure Policy, *supra*.

92. Under these circumstances, EPIC members have reasonably treated their SSA data as highly sensitive and have trusted SSA to do the same.

93. Members of EPIC have been injured through the deprivation of their statutory privacy rights. They reasonably fear and are emotionally distressed by the unauthorized disclosure,

aggregation, misuse, and mishandling of their sensitive personal data through Defendants' compilation and disclosure of the new State Citizenship Lists.

94. For example, Dr. Lorraine Kisselburgh is an EPIC member and U.S. citizen who lives in and is registered to vote in Indiana. She is a former professor and current faculty fellow and lecturer at a university in Indiana, where she specializes in technology, society, and privacy. She became an EPIC member because she is concerned about protecting privacy, freedom of expression, and democratic values in the information age.

95. Defendants' improper access to, disclosure of, and misuse of Dr. Kisselburgh's sensitive personal data has caused her and will cause her to feel acute emotional distress. This includes her anger at the government's careless and reckless mishandling of her personal data, her feeling of betrayal caused by the government's nonconsensual repurposing of her personal data to create an illegal citizenship list, and her fear that the compilation and disclosure of her personal data subject to ill-defined procedures and safeguards will increase her vulnerability to data theft and security breaches.

RETRIEVED FROM DEMOCRACYDOCKET.COM

96. These injuries were caused by Defendants, who are collecting, consolidating, and disclosing the personal information of Dr. Kisselburgh and other EPIC members in violation of the Social Security Act, the Privacy Act, and other applicable laws.

97. Dr. Kisselburgh and other EPIC members did not consent to the intergovernmental collection, consolidation, matching, or disclosure of their SSNs or other personal information, including disclosure to third-party states. Nor did they consent to this information being used for voting-related purposes. In fact, voter registration in Indiana (where Dr. Kisselburgh is registered) does not even require one to provide a SSN, but simply a valid state-issued driver's license or U.S. passport, which is used to verify residency and citizenship.

98. Yet, upon information and belief, Defendants have done all of these things or are planning to imminently do so. This intrusion upon EPIC members' sensitive personal information, and the unauthorized and unconsented compilation and disclosure of their data without their consent, is alarming and offensive—particularly because they were given no advance notice or opportunity to comment on Defendants' novel misuse of their personal information before it began, as the law requires, and because there is no way to opt out.

99. This intrusion is causing EPIC members to fear the consequences of providing information to their government and accessing public services in the future, has diminished EPIC members' trust in government, and is frustrating EPIC members' reasonable expectation of going about their private lives without the unconsented collection and disclosure of their personal data by the federal government.

RETRIEVED FROM DEMOCRACYDOCKET.COM

100. In addition to these privacy-related harms, EPIC members who are registered to vote in states that access the State Citizenship Lists are also at grave risk of suffering harms to their voting rights and right to participate in the political process as a result of Defendants' actions. In particular, the State Citizenship Lists purport to provide voter eligibility information, such as age, citizenship status, and state of residence, but Defendants' unauthorized and ill-considered effort to use the data for those purposes will lead to numerous false positives—that is, faulty indications that qualified, registered voters on a state's voter rolls are ineligible.

101. In addition to the other harms described herein, numerous EPIC members are at heightened risk for inaccurate inclusion or exclusion in Defendants' State Citizenship Lists and Portal and as a result are at heightened risk of suffering privacy injury, reputational injury, and injury to their voting rights.

102. For example, EPIC member Anthony Nel is a derived U.S. citizen and resident of Denton County, Texas.[2] He votes regularly and intends to continue doing so. He is one of many Texas voters whose voter registration was already wrongly cancelled by local election officials in Texas because of their use of the Modified SAVE system and its incorporation of SSA's unreliable citizenship data, both of which the State Citizenship Lists must utilize.

103. Ultimately, Nel provided Texas officials with proof of citizenship and, as a result, his registration was reinstated. However, Nel is concerned that he will continue to be wrongly identified as a non-citizen because the State Citizenship Lists utilize the same outdated information from SSA as Modified SAVE to determine citizenship.

104. If that happens, Nel likely will again be forced to prove his citizenship status to retain his voter registration. Being caught in such a cycle, with his voting rights on the line, is distressing to him. He feels compelled to regularly check his voter registration status to ensure it is not wrongly cancelled again. The prospect of wrongly being deprived of his voting rights, being labeled an illegal voter, and suffering the resultant legal and reputational consequences are deeply distressing to Nel.

RETRIEVED FROM DEMOCRACYDOCKET.COM

105. Further, members of EPIC who are legally registered voters, but whose information is included in the State Citizenship Lists with errors, included on the wrong list, or incorrectly excluded from their state, will suffer reputational harm. This harm will result from the dissemination of false or misleading information about them to third parties—specifically, information indicating that they are illegally registered to vote, a crime. EPIC members will be

[2] A derived U.S. citizen is a foreign-born child who automatically acquires U.S. citizenship through the naturalization of their parent(s) Under the Child Citizenship Act of 2000: children under 18 with at least one U.S. citizen parent (naturalized or birth) gain citizenship automatically if they reside in the U.S. as lawful permanent residents. 8 U.S.C. § 1431(a) (Immigration & Nationality Act § 320).

chilled from registering to vote or from voting if they fear being wrongly accused of criminal acts as a result.

Informational injuries to EPIC and its members

106. In addition, EPIC members have also suffered and will continue to suffer ongoing harm by being deprived of information concerning the collection, aggregation, and sharing of their data that Defendants were statutorily required to disclose in advance of taking action. For instance, they do not know: the policies and practices that Defendants or state entities are following (if any) to store, control access to, retain, and dispose of the data being consolidated in the citizenship lists; the policies and practices Defendants are following (if any) when compiling and using this data; the steps taken to ensure that these "procedures" are technically secure and results in accurate records; the procedures to contest, correct, or update the result of these "procedures"; or the policies and practices the Defendants are following (if any) in the disclosure of the results of these "procedures" to states. All of this information, and other related information, should have been provided to EPIC and its members through SORNs and Federal Register notices *before* Defendants began compiling their personal information.

RETRIEVED FROM DEMOCRACYDOCKET.COM

107. Without this information guaranteed by law, EPIC and its members cannot adequately understand how EPIC members' personal data is being consolidated, disclosed, or used by Defendants, take steps to safeguard their data and their voting rights, or protect themselves from consequences. They also lack the necessary information to be able to submit a request for an accounting of the disclosures of their records under 5 U.S.C. § 552a(c) or a request to review and, if necessary, amend their personal records under § 552a(d).

108. This lack of information is concerning and distressing to EPIC and its members. EPIC and its members seek this information to be able to determine the steps needed to protect

themselves and their right to vote, such as establishing credit monitoring, closely monitoring their voter registration, and preparing to respond to efforts to remove them from the rolls.

109. EPIC and its members have also been deprived of advance notice and the opportunity to participate in the process of determining how their personal data is being collected and used, including the right to comment in advance on Defendants' collection, compilation, storage, and sharing of data and the right to have those comments considered. Many EPIC members have submitted comments and provided testimony to the government on many issues related to privacy. For example, EPIC member Kisselburgh has submitted with colleagues numerous comments to federal agencies to advocate for enhanced privacy protections, including on how to balance privacy and accessibility in voting systems. EPIC and its members have also submitted comments specifically in response to system of records notices under the Privacy Act, and EPIC and its members would have liked to provide comments on Defendants''s compilation and transmission of State Citizenship Lists had they been given an opportunity.

RETRIEVED FROM DEMOCRACYDOCKET.COM

110. EPIC and its members would have submitted comments on any SORN Defendants published regarding its collection and new uses of this data—had Defendants complied with the Privacy Act—and intend to do so if Defendants comply in the future.

111. Defendants' unlawful and unauthorized aggregation of EPIC members' sensitive personal information and broad grant of unauthorized and unwarranted access has caused and will continue to cause EPIC members significant harm. Those harms include: intrusion on EPIC members' seclusion and invasion of their privacy; the loss of EPIC members' statutory privacy rights; the misuse and repurposing of EPIC members' private personal data in unauthorized ways; the sharing of EPIC members' personal data with unauthorized third parties with no lawful right to access it through unsecured means; EPIC members' highly reasonable unease and fears about it

being held by Defendants, including dissemination to third-party state entities; and EPIC members' unease and fears about bulk uploads and queries of their sensitive personal data. Over the last several months, EPIC has heard from members who are disturbed by and concerned about the federal government's efforts to create a massive "citizenship list."

112. EPIC members have been harmed by Defendants' compilation and disclosure of State Citizenship Lists, and will continue to suffer these and additional harms absent action by this Court to stop Defendants' illegal actions and require compliance with the law.

Injuries to EPIC as an organization

113. EPIC is also independently injured by Defendants' unlawful compilation, disclosure, and misuse of the personal data of millions of Americans.

114. EPIC is a leading privacy organization. Its mission is to protect the fundamental right to privacy, freedom of expression, and democratic values in the digital age for all people through advocacy, research, and litigation. Central to this mission is oversight and analysis of government activities that affect individual privacy. Among its activities, EPIC engages in advocacy, research, and public education about the collection, use, retention, and transfer of personal information by federal agencies, including large-scale databases and mass surveillance programs. EPIC also engages in research, advocacy, and public education concerning the privacy of the systems and databases used in immigration, Social Security Administration, and elections.

115. As part of its core mission, EPIC devotes significant resources to monitoring changes to the collection, use, retention, and transfer of personal information by state and federal agencies; educating the public about privacy and government oversight through events, social media, and other advocacy campaigns; and collaborating with partner organizations to advance the protection of privacy. EPIC devotes resources including funding, staff time, and strategic

RETRIEVED FROM DEMOCRACYDOCKET.COM

bandwidth to planning and executing this work. And EPIC serves a crucial role in informing peer civil society groups about state laws regarding privacy, civil liberties, and open government.

116. Defendants' unlawful efforts to compile, misuse, and share Americans' private information inflict multiple types of harm on EPIC and frustrate its ability to carry out its core functions.

117. First, Defendants' violations of the Privacy Act's notice requirement harm, and will continue to harm, EPIC. As detailed above, Defendants have not provided the statutorily required public notice (including through issuing SORNs) for the compilation and distribution of the State Citizenship Lists and the dissemination of data through the Portal.

RETRIEVED FROM DEMOCRACYDOCKET.COM

118. For decades, EPIC has relied extensively on information that the Privacy Act mandates agencies to disclose, including information in SORNs. 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 Freedom of Information Act requests for agency records. EPIC's ability to perform these mission-critical functions is directly impaired by Defendants' failure to publish statutorily required SORNs.

119. Defendants' actions here have frustrated, and will continue to frustrate, this aspect of EPIC's mission-critical work. For example, EPIC lacks key information that it would otherwise have available to it if Defendants had complied with their Privacy Act obligations, including: the identity of the system(s) which will be used to create and maintain the State Citizenship Lists and

related records; the purported legal authority for the establishment and maintenance of the relevant system(s) and State Citizenship Lists; the categories of records implicated; the sources of those records; the full range of proffered routine uses for which the State Citizenship Lists and related records may be disclosed; the procedures for verifying the accuracy of State Citizenship Lists; the policies and practices for the access, retrieval, verification, contesting, retention, and disposal of the relevant records; the administrative, technical, and physical safeguards in place to protect the relevant systems and records; and whether any statutory exemptions assertedly apply to the relevant system(s).

120. Without this vital information, EPIC is kept in the dark about exactly how its members' information and the information of millions of Americans is being used and the magnitude of the privacy risks to eligible naturalized, derived, and U.S.-born citizen registrants and voters. As a result, it cannot properly educate its members, the public, or the press about these risks and how to mitigate them.

RETRIEVED FROM DEMOCRACYDOCKET.COM

121. Moreover, EPIC has and will continue to expend resources to attempt to bridge the information gap created by Defendants' failure to abide by its notice obligations under the Privacy Act. EPIC must divert resources from its usual programs to expend them on alternate, more labor-intensive, and less comprehensive methods 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.

122. Accordingly, EPIC's ability to perform its mission-critical functions, including researching, educating, and advocating on issues impacting the privacy rights of its members and the public at large are directly impaired by Defendants' actions.

123. Second, EPIC has suffered, and will continue to suffer, harm resulting from Defendants' violation of the Privacy Act's notice-and-comment requirement. As part of its core mission, EPIC routinely submits comments on SORNs and matching agreement notices published in the Federal Register and other proposed agency actions related to information databases and mobilizes its members and partners to do the same. Here, it has been denied the statutorily guaranteed opportunity to comment in advance on Defendants' collection, compilation, and sharing of personal data.

124. Had Defendants complied with their statutory obligation to provide an opportunity to comment, EPIC could have raised concerns about the impact of DHS's actions on personal privacy, associated security risks, and the willingness of citizens to participate in aspects of civil life. EPIC also could have offered potential solutions to safeguard sensitive personal information in a manner that could be constructive to Defendants' policy goals while protecting privacy rights.

RETRIEVED FROM DEMOCRACYDOCKET.COM

125. Third, Defendants' unlawful misuse of private personal information disrupts, and will continue to disrupt, EPIC's existing privacy education and protection efforts. Defendants' actions hamper EPIC's ability to execute these mission-critical functions and necessitates the diversion of resources to address and attempt to mitigate these privacy violations—in service of its mission to promote digital privacy and public awareness of related issues.

126. For example, EPIC has received increased questions and inquiries about Defendants' actions and their impact on privacy, data security, and right to vote. Responding to these inquiries has forced EPIC to divert significant staff time away from other priorities.

127. Defendants' actions have also forced, and will continue to force, EPIC to expend staff and financial resources in other ways, including: investigating the processes by which the States Citizenship Lists will be compiled and disclosed; seeking (unsuccessfully) to identify

supporting agency documentation (including SORNs and privacy impact assessments) that by law must be made public; conferring with other experts; sharing intelligence and analysis with partner organizations and the press, who themselves have been deprived by Defendants of important information concerning the State Citizenship Lists; and developing resources relating to the compiling and transmission of State Citizenship Lists.

128. These efforts to mitigate the effects of Defendants' unlawful actions require EPIC to divert its resources, including the time and efforts of staff, away from existing priorities and programs. EPIC's other organizational priorities include consumer protection, surveillance oversight, platform governance, the preservation of human rights amid the proliferation of artificial intelligence, the adoption of robust privacy legislation and regulation, and the enforcement of consumer privacy laws. Expending greater resources to protect the privacy of millions of Americans put at risk by Defendants detracts from these and other programs aimed at safeguarding the fundamental right to privacy.

RETRIEVED FROM DEMOCRACYDOCKET.COM

129. Defendants' unlawful misuse of personal information thus thwarts EPIC's mission and undermines its core activities. EPIC has been and will be forced to expend more of its limited resources to educate individuals, the press, and civil society partner organizations about the uses and misuses of personal data held by federal agencies and the privacy risks posed by Defendants unlawfully compiling and transmitting State Citizenship Lists. EPIC will accordingly have fewer resources to devote to its existing core organizational activities.

CLAIMS FOR RELIEF

COUNT I
Violation of the APA
(Agency Action in Excess of Statutory Authority)

130. Plaintiff repeats and incorporates by reference each of the foregoing allegations as if fully set forth herein.

131. The APA requires courts to "hold unlawful and set aside agency action" that is "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).

132. DHS's Implementation Memo and Defendants' decision to create and disclose State Citizenship Lists and associated information pursuant to that memo are final agency actions for which there is "no other adequate remedy in a court," within the meaning of the APA. 5 U.S.C. § 704; *see Venetian Casino Resort, L.L.C. v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008) ("policy of disclosing confidential information without notice" is final agency action).

RETRIEVED FROM DEMOCRACYDOCKET.COM

133. An "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)).

134. No statute authorizes Defendants to create, maintain, or disclose lists of U.S. citizens for any purpose, including for the purpose of ensuring "integrity" in federal elections.

135. No statute authorizes Defendants to disclose hundreds of millions of U.S. citizens protected personal information to each other or state election officials.

136. DHS claims that 8 U.S.C. § 1373 supplies "statutory authority . . . to send and receive immigration status information to and from federal, state, and local government entities."

Ex. at 2. But neither this statute—nor any other statute—authorizes Defendants to create, maintain, send, request, receive, or disclose the State Citizenship Lists.

137. Defendants' acts are 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 Social Security Act)

138. Plaintiff repeats and incorporates by reference each of the foregoing allegations as if fully set forth herein.

139. The APA requires courts to "hold unlawful and set aside" agency action that is "not in accordance with law" or "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

140. The Social Security Act prohibits SSA from "disclosure" of "any file, record, report, or other paper, or any information" except as the SSA Commissioner "may by regulations prescribe" or "as otherwise provided by Federal law." 42 U.S.C. § 1306(a)(1); *see also* 20 C.F.R. § 401.135.

141. The Social Security Act further provides that "Social security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law enacted on or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such social security account number or related record." 42 U.S.C. § 405(c)(2)(C)(viii)(I).

142. Under SSA policy, the agency will disclose or "verify SSNs, and SSN information" only "under limited circumstances as allowed or required by Federal laws," where SSA has express "legal authority and where we are able to identify the true number holder." SSA Disclosure Policy,

RETRIEVED FROM DEMOCRACYDOCKET.COM

supra. Under that policy, for SSA to verify SSNs pursuant to a federal statute, "the statute must specifically mandate that SSA disclose SSNs." *Id.*

143. SSA policy further states SSA does "not have the legal authority to disclose information about U.S. citizens to DHS," and that "[i]f DHS requests information and we determine the information pertains to both U.S. citizens and aliens, only information about the aliens can be disclosed." *Id.*; *accord* SSA, POMS GN 03313.095, *supra*.

144. Section 2(a) of the 2026 Elections EO requires that State Citizenship Lists "shall be derived from," among other sources, "SSA records."

145. Likewise, the Implementation Memo confirms that State Citizenship Lists will include "information from . . . SSA." Ex. A at 2.

146. DHS claims authority to obtain SSA records under 8 U.S.C. § 1373, a statute enacted after October 1, 1990. Omnibus Consolidated Appropriations Act of 1997, Pub. L. No. 104-208 § 642, 110 Stat 3009, 3009–707.

147. SSA's disclosure of its records to DHS and to state election officials for State Citizenship Lists and related processes violates 42 U.S.C. § 1306(a)(1), because it is not authorized by any law.

148. DHS obtaining SSNs and related records from SSA pursuant to a statute enacted after October 1, 1990, violates 42 U.S.C. § 405(c)(2)(C)(viii)(I).

149. Defendants' actions therefore violate the Social Security Act and are "not in accordance with law" and "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

RETRIEVED FROM DEMOCRACYDOCKET.COM

COUNT III
Violation of the APA
(Agency Action Contrary to the Privacy Act - Failure to Provide Notice or an Opportunity for Public Comment)

150. Plaintiff repeats and incorporates by reference each of the foregoing allegations as if fully set forth herein.

151. The APA requires courts to "hold unlawful and set aside" agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law," or "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

152. The Privacy Act requires agencies to publish a SORN in the Federal Register whenever they "establish[] or revis[e]" a "system of records." 5 U.S.C. § 552a(e)(4). And at least 30 days before "any new use or intended use of the information in the system," the agency must "publish in the Federal Register notice" of the new use and "provide an opportunity for interested persons to submit written data, views, or arguments to the agency." *Id.* § 552a(e)(11).

153. "In no circumstance may an agency use a new or significantly modified routine use as the basis for a disclosure fewer than 30 days following *Federal Register* publication." OMB Circular No. A-108 at 7, 12. And agencies "shall" review and consider any "public comments on a published SORN." *Id*. at 7.

154. Through Defendants' State Citizenship Lists Portal, Defendants are compiling, collecting, maintaining, and disclosing highly sensitive data housed within DHS, SSA, and DOS, including at a minimum names, dates of birth, SSNs, and citizenship status.

155. Despite creating new systems of records and substantially modifying existing systems and their usage, Defendants failed to publish new or modified SORNs in the Federal Register relating to the State Citizenship Lists process, in violation of 5 U.S.C. §§ 552a(e)(4), (11).

RETRIEVED FROM DEMOCRACYDOCKET.COM

156. Defendants failed to publish in the Federal Register notice of "any new use or intended use of the information in the system" at least 30 days before such new use or intended use as required by 5 U.S.C. § 552a(e)(11).

157. Defendants also failed to "provide an opportunity for interested persons to submit written data, views, or arguments to the agency" regarding their use of the State Citizenship Lists data as required by 5 U.S.C. § 552a(e)(11).

158. The timeline and "phased delivery" set forth in DHS's Implementation Memo is facially inconsistent with the requirements of 5 U.S.C. §§ 552a(e)(4), (11). This confirms Defendants will compile and disclose State Citizenship Lists and associated information without complying with those legal requirements.

159. Defendants' actions therefore violate the Privacy Act and are "not in accordance with law" and "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

RETRIEVED FROM DEMOCRACYDOCKET.COM

COUNT IV
Violation of the APA
(Agency Action Contrary to the Privacy Act - Unauthorized Disclosure)

160. Plaintiff repeats and incorporates by reference each of the foregoing allegations as if fully set forth herein.

161. The APA requires courts to "hold unlawful and set aside agency action" that is "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)

162. The Privacy Act generally prohibits disclosure of an individual's records from a system of records without their consent unless it fits one of 13 exceptions. *See* 5 U.S.C. § 552a(b)(1)-(13).

163. Under the Implementation Memo, Defendants will consolidate USCIS, SSA, and DOS data through the State Citizenship Lists Portal, and will compile, create, and disclose State Citizenship Lists to states, all in violation of numerous provisions of the Privacy Act.

164. These disclosures, and the policies and agreements authorizing them, violate 5 U.S.C. § 552a(b). They are or will be made without the consent of the individuals whose information Defendants are disclosing, and they fall within no statutory exception or any properly noticed "routine use."

165. Defendants' actions therefore violate the Privacy Act and are "not in accordance with law" and "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

RETRIEVED FROM DEMOCRACYDOCKET.COM

COUNT V
Violation of the APA
(Arbitrary and Capricious Agency Action)

166. Plaintiff repeats and incorporates by reference each of the foregoing allegations as if fully set forth herein.

167. The APA requires courts to "hold unlawful and set aside agency action" that is "arbitrary" and "capricious." 5 U.S.C. § 706(2)(A).

168. DHS's Implementation Memo and Defendants' decision to create and disclose State Citizenship Lists and associated information pursuant to that memo are arbitrary and capricious because, among other things, the agencies departed from agency policy without acknowledgment or explanation; failed to consider public comments as the Privacy Act mandates; and failed to consider the privacy and data-security risks of their actions, the Federal Information Security Modernization Act's requirements for data security, the chilling effect their actions would have on Americans' voting rights, and the reliance interests and reasonable privacy expectations of the millions of Americans who never consented to their personal data being compiled in a

federal database rife with inaccuracies maintained by DHS and shared with states, or used to determine their eligibility to exercise their fundamental right to vote.

COUNT VI
Violation of the APA
(Agency Action Contrary to Constitutional Power)

169. Plaintiff repeats and incorporates by reference each of the foregoing allegations as if fully set forth herein.

170. The APA requires courts to "hold unlawful and set aside agency action … found to be . . . contrary to constitutional right, power, privilege, or immunity." 5 U.S.C. § 706(2)(B).

171. The Constitution presumes coequal branches, and the "doctrine of separation of powers" lies "at the heart of our Constitution." *Buckley v. Valeo*, 424 U.S. 1, 119 (1976).

172. The Executive cannot usurp Congress's legislative authority by fiat. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 585 (1952). The Executive has no constitutional power to enact, amend, or repeal parts of duly enacted statutes. *See Clinton v. City of New York*, 524 U.S. 417, 438–39 (1998).

173. There is a "direct interest in objecting to laws that upset the constitutional balance between the National Government and the States when the enforcement of those laws causes injury that is concrete, particular, and redressable. Fidelity to principles of federalism is not for the States alone to vindicate." *Bond v. United States*, 564 U.S. 211, 222 (2011).

174. The Constitution vests "the power to determine who is qualified to vote" in the States and "the power to regulate federal election procedures" in the States and Congress; the Constitution "assigns no direct role to the President in either domain." *League of United Latin Am. Citizens v. Exec. Off. of the President* (*LULAC*), 818 F. Supp. 3d 34, 59 (D.D.C. 2026); *see* U.S.

RETRIEVED FROM DEMOCRACYDOCKET.COM

Const. art. I, § 2, cl. 1 (Voter Qualifications Clause); *id.* amend. XVII; *id.* art. I, § 4, cl. 1 (Elections Clause); *see also Arizona v. Inter Tribal Council of Ariz., Inc.*, 570 U.S. 1, 17 (2013).

175. Here, no statute authorizes Defendants' creation or disclosure of State Citizenship Lists and associated information for purposes of verifying voter eligibility.

176. By acting with a "total absence of authority from Congress in a domain that the Constitution assigns to Congress and the States," *LULAC*, 818 F. Supp. 3d at 87, Defendants have violated the Constitution.

177. Defendants' actions are therefore "contrary to constitutional right, power, privilege, or immunity." 5 U.S.C. § 706(2)(B).

RETRIEVED FROM DEMOCRACYDOCKET.COM

COUNT VII
Violation of the Constitution's Separation of Powers, Federalism Principles, the Elections Clause, the Voter Qualifications Clause, and the 17th Amendment

178. Plaintiff repeats and incorporates by reference each of the foregoing allegations as if fully set forth herein.

179. This Court has inherent equitable power to enjoin unconstitutional Executive conduct. *See Free Enter. Fund v. Pub. Co. Acct. Oversight Bd.*, 561 U.S. 477, 491 n.2 (2010); *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320, 327 (2015).

180. For the same reasons set forth above in Count VI, Defendants' actions violate the Constitution and must therefore be enjoined and declared unlawful.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

1) Declare that DHS's Implementation Memo and Defendants' decision to create and disclose State Citizenship Lists—including but not limited to the State Citizenship Lists Portal and associated information—are unlawful, ultra vires, unconstitutional, and

arbitrary and capricious;

2) Hold unlawful, stay, vacate, and set aside DHS's Implementation Memo and Defendants' decision to create and disclose State Citizenship Lists, including but not limited to the State Citizenship Lists Portal and associated information;

3) Order Defendants and those in active concert or participation with Defendants to delete, disentangle, and unlink any State Citizenship Lists data (including State Citizenship Lists Portal data) in its possession, custody, or control;

4) Order Defendants to instruct any party it has provided State Citizenship Lists data (including State Citizenship Lists Portal data) to delete, disentangle, and unlink that data;

5) Order Defendants to publish all information and comply with all procedures mandated by the Privacy Act for the State Citizenship Lists data (including the State Citizenship Lists Portal data) it has already collected;

6) Enjoin Defendants from disclosing any State Citizenship Lists data (including the State Citizenship Lists Portal data) internally and to non-agency personnel, including to other federal agencies, state agencies, or private contractors;

7) Enjoin Defendants and those in active concert or participation with Defendants from using or in any way relying on any State Citizenship Lists data (including the State Citizenship Lists Portal data);

8) Grant any temporary, preliminary, or permanent injunctive relief necessary to prevent Defendants' actions from irreparably harming Plaintiffs;

9) Retain jurisdiction to ensure compliance with this Court's orders;

10) Award Plaintiffs their costs and reasonable attorneys' fees incurred in this action; and

11) Grant any other relief this Court deems just and proper.

RETRIEVED FROM DEMOCRACYDOCKET.COM

Dated: August 31, 2026

Respectfully submitted,

Nikhel S. Sus (Bar No. 31090)
John B. Hill*
Reuven Dashevsky*
CITIZENS FOR RESPONSIBILITY
AND ETHICS IN WASHINGTON
P.O. Box 14596
Washington, DC 20044
(202) 408-5565
nsus@citizensforethics.org
jhill@citizensforethics.org
rdashevsky@citizensforethics.org

John Davisson*
Mayu Tobin-Miyaji*
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, D.C. 20036
(202) 483-1140
davisson@epic.org
tobin-miyaji@epic.org

R. Orion Danjuma*
Julia L. Torti*
PROTECT DEMOCRACY PROJECT
82 Nassau Street, #601
New York, NY 10038
(202) 579-4582
orion.danjuma@protectdemocracy.org
jules.torti@protectdemocracy.org

Sara Chimene-Weiss*
PROTECT DEMOCRACY PROJECT
7000 N. 16th Street, Suite 120, #430
Phoenix, AZ 85020
(202) 934-4237
sara.chimene-weiss@protectdemocracy.org

Jane Bentrott*
Shelby Teeter*
PROTECT DEMOCRACY PROJECT
2020 Pennsylvania Ave. NW, Suite #163
Washington, DC 20006
(202) 579-4582
jane.bentrott@protectdemocracy.org
shelby.teeter@protectdemocracy.org

Counsel for Plaintiff

* *Pro hac vice* motion forthcoming