

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

ELECTRONIC PRIVACY INFORMATION
CENTER,

Plaintiff,

v.

U.S. CITIZENSHIP AND IMMIGRATION
SERVICES, *et al.*,

Defendants.

Case No. 8:26-cv-03457-PX

PLAINTIFF'S MEMORANDUM OF LAW IN SUPPORT OF ITS
MOTION FOR PARTIAL SUMMARY JUDGMENT

TABLE OF CONTENTS

INTRODUCTION	1
BACKGROUND	2
I. Relying on False Claims of Non-Citizen Voting and Fraud, the 2026 Elections EO Mandates the Creation and Distribution of Federal “State Citizenship Lists.”	3
II. DHS’s Implementation of Section 2 of the 2026 Elections EO Is Facially Unlawful.	4
III. The 2026 Elections EO Directs Defendants to Compile the State Citizenship Lists from Legally Protected Data Sources that Are Concededly Unreliable for these Purposes.	5
IV. A Similar Database-Creating Effort Was Vacated, but the 2026 Elections EO Implementation Memo Remains in Effect.....	6
LEGAL STANDARD.....	8
ARGUMENT.....	8
I. Plaintiff Challenges Final Agency Action.	8
II. The Implementation Memo and the “Course of Action” It Approves Violate the Privacy Act (Count III).	10
A. The Implementation Memo’s approved “course of action” is contrary to the Privacy Act’s notice-and-comment requirements.	12
B. The Implementation Memo’s deferred creation of the Portal’s “transparency and redress” functions facially violates the Privacy Act.....	14
III. The Implementation Memo is Contrary to the Privacy Act’s Restrictions on Disclosure (Count IV).....	15
IV. The Implementation Memo Is Contrary to the Social Security Act’s Restrictions on Disclosure (Count II).	16
V. The Implementation Memo Exceeds DHS’s Statutory Authority (Count I).	17
VI. EPIC Has Standing to Challenge DHS Defendants’ Illegal Actions.....	21
A. EPIC has associational standing.	22
B. EPIC has informational standing.	26

C.	EPIC and its members have procedural standing.	27
D.	The other elements of standing are satisfied.....	28
VII.	Plaintiff Is Entitled to its Requested Relief.....	28
A.	The Court should set aside the Implementation Memo and associated actions.....	28
B.	In the alternative, the Court should issue a permanent injunction.....	29
C.	The Court should declare the Defendants’ challenged actions unlawful.	30
CONCLUSION.....		30

INTRODUCTION

The American public trusts the federal government with vast troves of their most sensitive information. Congress, recognizing the danger posed by misuse or disclosure of this information, has passed several, mutually reinforcing statutes restricting agencies' ability to use, repurpose, and disclose Americans' data—both within the federal government and beyond it. But the Trump Administration, intent on inserting the executive branch in the business of election administration in defiance of our constitutional structure, has twice issued Executive Orders directing federal agencies to illegally compile, repurpose, and disclose their voluminous and disparate datasets to create admittedly inaccurate “lists” designed to exert executive control over voter eligibility and state election administration. This is as unprecedented as it is unlawful.

Accordingly, a federal district court has already held that the executive's consolidation and disclosure of sensitive Social Security Administration (SSA) data to the Department of Homeland Security (“DHS”) and States—through modifications to the Systematic Alien Verification for Entitlements (“SAVE”) system—lacked any statutory authorization and violated the Social Security Act, Privacy Act, and Administrative Procedure Act (“APA”). Now DHS—in concert with SSA, Department of State (“DOS”), and United States Citizenship and Immigration Services (“USCIS”)—is again compiling sensitive data, across multiple federal agencies that handle Americans' most sensitive information, to create “State Citizenship Lists.” Their goal is to create a master list of every “verified” adult U.S. citizen and their state of residence, which the Administration will use to operationalize its purported “election integrity” initiatives.

But Congress has not authorized the federal government to create these “State Citizenship Lists.” Nor does the government possess any dataset capable of providing accurate, real-time verification of U.S. citizenship status or state of residence. And in scrambling to implement this

plan, the DHS Defendants¹ are violating critical safeguards of the Privacy Act, Social Security Act, and APA, and far exceeding their statutory authority. Worse still, DHS plans to imminently distribute those Lists to state election administrators across the country, further flouting those same laws. Plaintiff, a national privacy rights organization whose members and mission are directly harmed by Defendants' illegal actions, asks this Court to vacate DHS's memorandum adopting this course of action in order to protect millions of Americans' privacy and voting rights.²

BACKGROUND

The Constitution gives authority over election administration largely to the States, and no authority at all to the federal executive branch. U.S. Const. art. I, § 2, cl. 1; *id.* amend. XVII; *id.* art. I, § 4, cl. 1. Nonetheless, President Trump relentlessly has sought to seize control over elections. This has taken many forms, including multiple failed attempts at passing legislation, publicly claiming power over election administration, and spreading lies about non-citizen voting. *See* Hill Decl. ¶¶ 2–3, 6–7, Exs. C, D. President Trump has also issued two executive orders aimed at federalizing election administration: (1) a March 25, 2025 executive order titled *Preserving and Protecting the Integrity of American Elections* (the “2025 Elections EO”), Executive Order No. 14248, 90 Fed. Reg. 14005 (Mar. 25, 2025) (Hill Decl. ¶ 9, Ex. F); and (2) a March 31, 2026 executive order titled *Ensuring Citizenship Verification and Integrity in Federal Elections* (the “2026 Elections EO”), Executive Order No. 14399, 91 Fed. Reg. 17125 (March 31, 2026) (Hill Decl. ¶ 5, Ex. B). Plaintiff challenges agency approval of a course of action to implement Section

¹ As used here, the term “DHS Defendants” includes DHS, the DHS Secretary, USCIS, and the USCIS Director.

² Plaintiff moves for summary judgment as to Counts I–IV of its Complaint, and only with respect to DHS's June 8 Implementation Memo. Plaintiff does not move at this time as to other final agency actions challenged in the Complaint or as to Counts V–VII, the resolution of which may require production of an administrative record or discovery. However, if the Court grants this motion on any count, it may dismiss the remaining claims without prejudice as “prudentially moot” and enter final judgment. *See CREW v. OMB*, 791 F. Supp. 3d 29, 59 (D.D.C. 2025) (citing cases).

2(a) of the 2026 Elections EO, which was finalized in a memorandum signed by DHS Secretary Mullin. *See* Hill Decl. Ex. A.

I. Relying on False Claims of Non-Citizen Voting and Fraud, the 2026 Elections EO Mandates the Creation and Distribution of Federal “State Citizenship Lists.”

Section 2(a) of the 2026 Elections EO mandates that (1) DHS, USCIS, and SSA share data to create for each State a “State Citizenship List” of individuals those agencies believe are citizens who will be above age 18 on election day and who reside in that State; (2) the State Citizenship Lists be sent to States’ chief election officials “no fewer than 60 days before each regularly scheduled Federal election”;³ and (3) the DHS Secretary create processes for individuals and States to propose changes, corrections, or updates to the Lists. *See* 2026 Elections EO § 2(a), Hill Decl. Ex. B at 1. The State Citizenship Lists are to be compiled from “citizenship and naturalization records, SSA records, SAVE data, and other relevant Federal databases.” *Id.*

Section 2(b) expressly threatens that the Attorney General will prioritize investigation and prosecution of any “State and local officials” who “issue Federal ballots to individuals not eligible to vote in a Federal election.” *Id.* § 2(b), Hill Decl. Ex. B. at 2; *see also id.* § 5, Hill Decl. Ex. B at 3. Section 2(b) defines “eligible to vote in a Federal election” as having the same characteristics as individuals on the State Citizenship Lists. *Id.* § 2(b), Hill Decl. Ex. B at 2. The risk of facing a “priority” federal investigation—even one that is not ultimately successful or meritorious—places enormous coercive pressure on States to integrate the State Citizenship Lists into their election administration processes. *See id.*; *see also id.* § 5, Hill Decl. Ex. B at 3 (further threatening States and localities with federal funding cuts for any “noncompliance with Federal law”). That, of

³ As contemplated in the 2026 Elections EO, this date would have been September 4, 2026 for the November 3, 2026 midterm elections. However, after a September 2, 2026 conference with Plaintiff’s counsel, Defendants’ counsel represented that “The DHS citizenship data portal will not go live September 4 and [Defendants] will give plaintiffs 48 hours’ notice before it does.” Hill Decl. ¶ 24, Ex. AA.

course, is exactly the Trump Administration’s aim in mandating the creation of these lists in an executive order that has the stated purpose of “ensuring citizenship verification and integrity in federal elections.”

II. DHS’s Implementation of Section 2 of the 2026 Elections EO Is Facially Unlawful.

On June 8, 2026, Secretary Mullin signed and approved a plan, adopting it “as DHS’s primary means of implementing” the 2026 Elections EO. *See* Hill Decl. Ex. A at 5 (“Implementation Memo”). The Memo outlines a two-step process for implementing Section 2(a): (1) the creation of a “portal,” and (2) the creation and dissemination of State Citizenship Lists. *Id.* at 2–3. This “course of action,” *id.* at 1, is unlawful.

The Implementation Memo first commits DHS to creating a “federated portal” (the “Portal”) through which “state election officials . . . will be able to download separate outputs from USCIS, SSA, and DOS.” *Id.* at 2. “The downloaded files will provide citizenship related data elements, such as name, date of birth, and relevant agency identifiers.” *Id.* For SSA, the “relevant agency identifier[]” is an SSN. *See* Hill Decl. ¶¶ 19–20, Exs. V, W. The Implementation Memo also commits to “delivering” the Portal and “enabling States to access citizenship related data” no later than the deadline “directed by EO 14399.” *See* Hill Decl. Ex. A at 3–4; *supra* note 3.

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.” Hill Decl. Ex. A 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.*

The Implementation Memo states that “DHS will continue to work to generate from the information contained in this portal” consolidated State Citizenship Lists “to provide state election

officials no fewer than 60 days before each regularly scheduled Federal election.” *Id.* DHS Secretary Mullin has indicated that state election officials who refuse to use the State Citizenship Lists ahead of the November election will face investigation, fines, and even imprisonment. *See* Hill Decl. ¶ 13, Ex. P. In addition, Defendants’ representations in court filings confirm their commitment to distribute the State Citizenship Lists for use in the November 2026 election. *See* Application for a Stay at 27, *Trump v. California*, 2026 WL 2473573 (No. 26A124) (U.S. July 27, 2026) (arguing that “[a]bsent a stay” of the injunction of Section 2(a) and other provisions of the EO—which was later granted—“the government will be unable . . . to ensure voter integrity in the upcoming November 2026 election”).

III. The 2026 Elections EO Directs Defendants to Compile the State Citizenship Lists from Legally Protected Data Sources that Are Concededly Unreliable for these Purposes.

The State Citizenship Lists must be compiled from “citizenship and naturalization records, SSA records, SAVE data, and other relevant Federal databases.” Hill Decl. Ex. A at 1. But none of these data sources can reliably verify citizenship, let alone state of residence, for purposes of determining voter eligibility.

As for SSA data, SSA has 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.” Hill Decl. ¶ 11, Ex. N at 2. 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. Hill Decl. Ex. N at 3. SSA’s citizenship data is also incomplete for individuals older than 45 because “SSA did not begin to consistently maintain citizenship information until 1981.” Hill Decl. Ex. N at 2.

As for SAVE data, DHS has likewise acknowledged data gaps in its SAVE system, which relies heavily on SSA’s citizenship data. *See* Hill Decl. ¶ 10, Ex. G at 19 (warning SAVE “may share inaccurate information with registered agencies” and “may produce inaccurate results”), Ex. H at 17 (warning “[s]hortfalls in data accuracy in the system could cause incomplete or false results”). DHS has also confirmed that SAVE’s data gaps are especially likely to impact citizens born outside of the United States. Hill Decl. Ex. G at 15, Ex. I at 16; *see also* Hill Decl. ¶ 21, Ex. X at 2. Moreover, the federal government simply does not maintain up-to-date information on the state residency of its citizens. *See e.g., Husted v. A. Philip Randolph Inst.*, 584 U.S. 756, 765 (2018) (USPS’s National Change of Address Database not an accurate source of state residency information); Hill Decl. ¶ 23 (describing inaccuracy of IRS’s address data).

IV. A Similar Database-Creating Effort Was Vacated, but the 2026 Elections EO Implementation Memo Remains in Effect.

A court has already vacated a remarkably similar scheme—undertaken to implement the 2025 Elections EO—based on claims similar to those Plaintiff advances in this case. 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.” Hill Decl. Ex. F at 1–2. It also directs SSA to make its databases available “to all State and local election officials” for “verifying” voter eligibility. *Id.* at 3. To implement these directives, DHS and SSA haphazardly made major changes to a USCIS immigration database designed to run queries on *non*-citizens, known as the “SAVE” system. For the first time, DHS directly linked SAVE to SSA’s Master File (also known as NUMIDENT) of SSN holders, a highly sensitive database with information on “over 300 million” U.S. citizens, including SSNs, other identifying numbers, names, dates and places of birth, citizenship indicators,

and death records. Hill Decl. ¶ 10, Ex. M at 1; *see also* Notice of Modified System of Records, 90 Fed. Reg. 10025, 10026 (Feb. 20, 2025).

On June 22, 2026, a federal court held unlawful, vacated, and set aside DHS’s and SSA’s 2025 modifications to the SAVE system. *See League of Women Voters v. DHS*, 2026 WL 1784297, at *2 (D.D.C. June 22, 2026), *appeal docketed*, No. 26-5243 (D.C. Cir. June 29, 2026) (“*LWV*”). The court held the SAVE modifications and the inter-agency data disclosures they enabled violated the Social Security Act and the Privacy Act; were arbitrary and capricious under the APA; and lacked statutory authorization. *Id.* at *20–33. The court explicitly rejected DHS’s and SSA’s position that 8 U.S.C. § 1373 authorizes the agencies to freely disclose citizen status information to each other and to States. *Id.* at *32–33. Notably, the Implementation Memo at issue in this case claims that the expansive inter-agency data disclosure it requires is *also* authorized by 8 U.S.C. § 1373. *See* Hill Decl. Ex. A at 2.

Multiple lawsuits have directly challenged the 2026 Elections EO, and one court enjoined implementation of Section 2 as to 23 States and the District of Columbia until that injunction was stayed by the Supreme Court on August 24, 2026. *See Trump v. California*, 2026 WL 2473573 (U.S. Aug. 24, 2026) (staying the injunction on standing and ripeness grounds— where plaintiffs had filed suit before the Implementation Memo was adopted—because the “prediction” plaintiffs had made as to “how the Executive Branch might eventually implement” § 2(a) was “no more than conjecture” at the time of filing, while noting “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” (cleaned up)). Thus, there is no court order now in effect that remedies the illegality of the Defendants’ adoption of a course of action to implement Section 2 of the EO.

LEGAL STANDARD

APA claims “are properly decided on summary judgment,” but the standard set forth in Federal Rule of Civil Procedure 56 governing factual disputes does not apply. *Deese v. Esper*, 483 F. Supp. 3d 290, 303–04 (D. Md. 2020) (citations omitted). In APA cases, “[s]ummary judgment . . . serves as the mechanism for deciding, as a matter of law, whether the agency action is . . . consistent with the APA standard of review.” *Stuttering Found. of Am. v. Springer*, 498 F. Supp. 2d 203, 207 (D.D.C. 2007). “The ‘entire case’ on review is a question of law.” *Am. Bioscience, Inc. v. Thompson*, 269 F.3d 1077, 1083 (D.C. Cir. 2001). And where “a party presents purely legal contrary-to-law claims divorced from arbitrary-and-capricious claims,” the court can rule on the merits of the claim without the administrative record. *Quarcoo v. Edlow*, 2026 WL 2491214, at *15 (D. Md. Aug. 25, 2026). A “motion for summary judgment may be filed at any time . . . even as early as commencement of the action.” *Atrium Corp. Cap. Ltd. v. Williams*, 2023 WL 8282769, at *2 n.3 (D.S.C. 2023) (citing Fed. R. Civ. P. 56(b)).

ARGUMENT

I. Plaintiff Challenges Final Agency Action.

DHS’s Implementation Memo and the “course of action” it approves, Hill Decl. Ex. A at 1, constitute “final agency action” subject to APA review because they “mark the consummation of the agency’s decisionmaking process” and are actions by “which rights or obligations have been determined, or from which legal consequences will flow.” *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997) (cleaned up).

DHS’s Implementation Memo is formally signed by Secretary Mullin himself, expressly “approv[ing] a course of action for U.S. Citizenship and Immigration Services (USCIS) that relates to implementing Section 2(a) of Executive Order (EO) 14399,” and which “rescinds and supersedes” previous memoranda. Hill Decl. Ex. A at 1. This formal approval by the Department

head is surely a consummation of DHS’s decisionmaking process sufficient to satisfy the first prong of *Bennett*. See *Village of Bald Head Island v. U.S. Army Corps. of Eng’rs.*, 714 F.3d 186, 193, 195 (4th Cir. 2013) (holding formal approval of agency project was a final agency action); *League of Women Voters of U.S. v. USCIS*, --- F. Supp. 3d ----, 2026 WL 2224637 at *23 (D. Md. 2026) (“actions are final when there is nothing further for the agencies to do to formalize the decisions” (cleaned up)).

DHS’s Implementation Memo also determines the obligations of the DHS Defendants *and* the rights of those whose information is being disclosed, plainly satisfying *Bennett*’s second prong. See *Doe v. Tenenbaum*, 127 F. Supp. 3d 426, 461 (D. Md. 2012). The Implementation Memo commits the DHS Defendants to the creation of the Portal that “must be made available to federal, state, and local agencies” and through which “state election officials . . . will be able to download separate outputs from USCIS, SSA and DOS.” Hill Decl. Ex. A at 2. It further directs them 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 3. This alone is enough. See *Phila. Yearly Meeting of Religious Soc’y of Friends v. DHS*, 2026 WL 280089 at *3 (D. Md. Feb. 3, 2026) (holding that DHS memorandum adopting policy was final agency action because it determined DHS’s “own rights or obligations”).

As part of these efforts, the Implementation Memo directs the transmission of citizenship-status information between DHS, SSA, DOS, and the States. This policy of disclosure imposes tangible legal consequences on EPIC’s members who have had their confidential data disclosed in violation of federal law. See *Venetian Casino Resort, L.L.C. v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008) (“policy of . . . disclos[ing] confidential information without notice is surely . . . one by

which the submitter’s rights and the agency’s obligations have been determined” (cleaned up)); *LWV*, 2026 WL 1784297, at *19 (same, concerning SAVE); *AFSCME v. SSA*, 771 F. Supp. 3d 717, 788–89 (D. Md. 2025) (same, concerning DOGE).

II. The Implementation Memo and the “Course of Action” It Approves Violate the Privacy Act (Count III).

The Implementation Memo approves a course of action that is facially inconsistent with the Privacy Act’s procedural safeguards and substantive restrictions.⁴

The Privacy Act imposes “strict notice and comment requirements.” *LWV*, 2026 WL 1784297, at *4. 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. 5 U.S.C. § 552a(e)(4). And 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) (emphasis added).

Examples of “significant changes” 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

⁴ APA review and relief are available for Defendants’ violations of the Privacy Act. *See, e.g., Sackett v. EPA*, 566 U.S. 120, 128 (2012) (“The APA . . . creates a ‘presumption favoring judicial review of administrative action.’”); *Doe v. Chao*, 540 U.S. 614, 619 n.1 (2004) (“inattention” of Privacy Act to “standards of proof governing equitable relief” may be explained by APA’s “general provisions for equitable relief”); *Doe v. Chao*, 435 F.3d 492, 505 n.17 (4th Cir. 2006) (“Often . . . injunctive relief for a Government’s violation of the [Privacy] Act will instead be appropriate and authorized by the APA.”); *see also LWV*, 2026 WL 1784297, at *21–23.

existing routine use that has the effect of expanding the availability of the information in the system.” OMB, Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act* 5–6 (2016), <https://perma.cc/N9QK-SDLE>.

“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.” *Id.* at 7, 12. And agencies “shall” review and consider any “public comments on a published SORN.” *Id.* at 7.

“The Privacy Act’s public notice and comment structure is an essential component of the Act and an essential piece of American democracy,” and it embodies the principle that “Americans deserve to know the nature, scope, and routine uses of the records *before* they are collected by the federal government.” *LWV*, 2026 WL 1784297, at *27 (quoting *United States v. Weber*, 816 F. Supp. 3d 1168, 1194 (C.D. Cal. 2026)). “Indeed, ‘it is flatly inconsistent with the text, structure, and purpose of the Privacy Act for an agency to initiate a major new data-sharing program affecting the sensitive data of millions of Americans, then validate that program as a ‘routine use’ months after it has begun.’” *Id.* (quoting *League of United Latin Am. Citizens v. EOP* (“*LULAC*”), 818 F. Supp. 3d 34, 115–16 (D.D.C. 2026)).

DHS’s Implementation Memo, which remains in effect and has not been rescinded, facially violates these “essential” requirements in two ways: (1) it adopts a course of action for establishing the Portal and DHS’s State Citizenship List-making process that is inconsistent with the Privacy Act’s notice-and-comment requirements, and (2) it defers creating “transparency and redress” mechanisms for individuals to access and correct their records until *after* the Portal goes live. Each defect is fatal and requires vacatur of the Implementation Memo as “not in accordance with law” and “without observance of procedure required by law.” 5 U.S.C. §§ 706(2)(A), (D).

A. The Implementation Memo’s approved “course of action” is contrary to the Privacy Act’s notice-and-comment requirements.

The Implementation Memo approves a “course of action” to compile “information under the control of” USCIS, SSA, and DOS in the Portal, Hill Decl. Ex. A at 1, and for DHS to “continue to work to generate from the information contained in this portal a consolidated list of United States citizens and residents” to send to state election officials prior to each federal election, *id.* at 3. But, as Defendants recognize, before doing so they must first have complied with the Privacy Act’s requirements for SORNs. *See id.* at 2, 3. They have not done so here.

According to the Implementation Memo, Defendants’ position is they comply with the Privacy Act by relying on “*existing*” SORNS that purportedly permit USCIS, SSA, and DOS to disclose citizenship data for the purpose of creating the State Citizenship Lists. *Id.* at 3 (emphasis added); *see also id.* (stating Defendants intend to rely on “*existing* legal authorities and *published* SORNs” (emphasis added)). But as of the time of this filing, no operative SORNs permit these routine uses, and no SORNs include DHS compiling citizenship data from SSA and DOS for voter verification purposes or making that information available to state election administrators. Thus, DHS’s course of action—which relies on non-existent SORNs—necessarily violates the Privacy Act’s requirements that they issue a SORN 30 days *before* effectuating any new “intended” routine use. *See* 5 U.S.C. §§ 552a(e)(4), (11).

Start with DHS and USCIS. On October 31, 2025, DHS issued a revised SORN for the SAVE system that included a new routine use permitting information sharing between USCIS, SSA, and other federal agencies for the purposes of verifying the citizenship of voters and added record source categories including (1) SSA’s Master Files of SSN holders, or NUMIDENT, and (2) DOS’s passport and Visa Record. *See* Notice of Modified System of Records, 90 Fed. Reg. 48948–49, 48953–54 (Oct. 31, 2025). But the 2025 DHS SAVE SORN is specific to the SAVE

system—nothing in it suggests DHS intends to create a *new* Portal to make State Citizenship Lists available to state election administrators. *Id.* And more importantly, on June 22, 2026, the 2025 DHS SAVE SORN was “set[] aside” and “vacate[d],” meaning the 2025 DHS SAVE SORN was “eliminated and replaced by any preexisting rule it had superseded.” *LWV*, 2026 WL 1784297, at *35 (quoting *Ctr. for Biological Diversity v. Haaland*, No. 22-cv-3588, 2023 WL 5161741, at *7 (D.D.C. Aug. 11, 2023)); *see also Griffin v. HM Fla.-ORL, LLC*, 144 S. Ct. 1, 2 n.1 (2023) (Kavanaugh, J., concurring) (when agency action is “set aside” under the APA, “the disapproved agency action is treated as though it had never happened.” (citation omitted)). The previous SORN for the SAVE system does not include any routine uses related to voter verification or collecting data from SSA or DOS, nor does it identify SSA or DOS among SAVE’s record source categories. *See generally* Notice of Modified System of Records, 85 Fed. Reg. 31798 (May 27, 2020). In other words, as of this filing, no DHS SORN contemplates DHS compiling and transmitting citizenship records from SSA and DOS.

The same is true for SSA. On November 12, 2025, SSA issued a revised SORN for its NUMIDENT system purporting to permit SSA to disclose SSA data regarding “citizenship and immigration status” to DHS. Notice of Modified System of Records, 90 Fed. Reg. 50879–80, 50883 (Nov. 12, 2025). But that SORN, like DHS’s corresponding SORN, was set aside and vacated on June 22. *LWV*, 2026 WL 1784297, at *35. As a result, as of this filing, no operative SSA SORN contemplates SSA sharing its citizenship records with DHS.

Nor does DOS have any SORN recognizing data sharing with DHS for voter verification purposes. *See* Notice of Modified System of Records, 86 Fed. Reg. 61822–25 (Nov. 8, 2021) (only permitting disclosure of DOS visa records to DHS for certain purposes that do not include voter

verification); Notice of Modified System of Records, 76 Fed. Reg. 39466, 39467 (July 6, 2011) (same but for DOS passport records).

Thus, no existing SORN contemplates the compilation and creation of State Citizenship Lists or sharing any related data through the Portal. And the timeline prescribed by the Implementation Memo—*i.e.*, distribution of the State Citizenship Lists 60 days prior to each election, meaning September 4 (tomorrow) for the upcoming November 3 midterm elections—leaves no doubt that Defendants’ approved course of action is contrary to the Privacy Act’s SORN requirements, including notice-and-comment 30 days prior to a “new” or “intended” routine use. 5 U.S.C. §§ 552a(e)(4), (11).

To the extent Defendants now argue the Memo’s deadlines have been superseded by their unofficial, out-of-court statements, Hill Decl. Ex. AA, they miss the point. Defendants have already failed to provide notice and an opportunity to comment through the issuance of a SORN prior to having adopted a new “intended use” of the information in their preexisting systems of records, as they did in the Implementation Memo. Moreover, DHS’s commitment to provide only 48 hours’ notice before publishing the Portal likewise facially violates the Privacy Act’s notice-and-comment requirements. *See id.* §§ 552a(e)(4), (11) (requiring 30 days notice and opportunity to comment in advance of new or intended new routine use becoming operational).

B. The Implementation Memo’s deferred creation of the Portal’s “transparency and redress” functions facially violates the Privacy Act.

The Privacy Act requires agencies to 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) (SORN must include, among other things, “the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content”); *id.* §

552a(e)(11) (requiring 30 days advance notice and consideration of public comments before new or modified systems go into effect); *see also* Privacy Act of 1974 § 2(b)(1)–(3), 88 Stat. 1896 (codified at 5 U.S.C. § 552a note) (listing transparency and records correction functions among the Act’s “purpose[s]”).

DHS’s Implementation Memo improperly inverts this statutory sequence: it defers creation of a “transparency and redress function” by which citizens can “view their own records and submit corrections” until an unspecified date *after* DHS’s separate listmaking begins, *after* the Portal goes live, and *after* the 2026 General Election. *See* Hill Decl. Ex. A at 3. And it erroneously frames these transparency and redress functions as a “follow-on enhancement,” rather than a statutory precondition to launching the Portal. *Id.* at 4. In these respects, the Memo is facially inconsistent with 5 U.S.C. §§ 552a(e)(4)(H), (11).

III. The Implementation Memo is Contrary to the Privacy Act’s Restrictions on Disclosure (Count IV).

The Privacy Act “prohibits, as a general matter, federal agencies from disclosing ‘any record’ of an individual in an agency ‘system of records’ without that individual’s consent.” *Doe v. Chao*, 511 F.3d 461, 463 (4th Cir. 2007). This general prohibition is subject to 13 statutory exceptions. *See* 5 U.S.C. § 552a(b); *see also Fattahi v. ATF*, 328 F.3d 176, 178 (4th Cir. 2003). None of these exceptions apply to the disclosures approved by the Implementation Memo, and the Implementation Memo cites none.⁵

⁵ Elsewhere, DHS has attempted (unsuccessfully) to justify similar disclosures by invoking the “routine use” exception. *See LWW*, 2026 WL 1784297, at *23–25 (rejecting applicability of “routine use” exception in similar circumstances). To qualify as a routine use, an agency’s disclosure must satisfy two conditions: it must (1) “be compatible with the purpose for which the agency collected the personal information,” and (2) “be in accordance with a routine use the agency has published in the Federal Register”—*i.e.*, a SORN. *Fattahi*, 328 F.3d at 178 (citing 5 U.S.C. §§ 552a(a)(7), (e)(4)(D)). The Implementation Memo’s disclosures satisfy neither. Disclosing the records of hundreds of millions of Americans to “[e]nsur[e] [c]itizenship [v]erification and [i]ntegrity in [f]ederal [e]lections,” Hill Decl. Ex. A at 1, is not compatible with the purposes for which DHS, SSA, or DOS have collected these records, *cf. LWW*, 2026 WL 1784297, at *24, and no SORN permits this as a routine use, *supra* Argument § II.A.

Because DHS’s Implementation Memo approves a course of action of disclosing hundreds of millions of Americans’ sensitive personal records without consent and without qualifying under any statutory exception, it violates 5 U.S.C. § 552a(b). The Memo should therefore be vacated as “not in accordance with law” and “without observance of procedure required by law.” 5 U.S.C. §§ 706(2)(A), (D).

IV. The Implementation Memo Is Contrary to the Social Security Act’s Restrictions on Disclosure (Count II).

The Implementation Memo approves a course of action under which DHS will necessarily violate one of the Social Security Act’s bedrock prohibitions on disclosure. That provision prohibits any “authorized person” 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). An “authorized person” includes “an officer or employee of the United States.” *Id.* § 405(c)(2)(C)(viii)(III). And “‘related record’ means any record, list, or compilation that indicates, *directly or indirectly*, the identity of any individual” with an SSN. *Id.* § 405(c)(2)(C)(viii)(IV) (emphasis added).

The Implementation Memo makes clear that, through the Portal, DHS will both obtain and disclose SSA records—including SSNs and “related records”—pursuant to a law enacted after October 1, 1990. The Memo says DHS’s Portal will be a “technological mechanism ... to provide States with citizenship list information from ... SSA,” via “downloaded files” with “citizenship related data elements, such as name, date of birth, and relevant agency identifiers.” Hill Decl. Ex. A at 2. For SSA, SSNs are the “relevant agency identifiers” that DHS’s Portal will disclose to States. *See* Hill Decl. Ex. V at 1. Separately, DHS will “generate from the information contained in this [P]ortal”—including SSA records—“a consolidated list of United States citizens and residents of the applicable State to provide to state election officials.” Hill Decl. Ex. A at 3. And

DHS claims it has “statutory authority” to take these actions “under 8 U.S.C. § 1373,” a statute enacted in 1996. *Id.* at 2; *see infra* § V.

Thus, “[t]here can be no question” that the Implementation Memo, on its face, directs disclosures in violation of § 405(c)(2)(C)(viii)(I). *See LWW*, 2026 WL 1784297, at *20 (so holding with respect to the Modified SAVE system). The Memo must therefore be vacated as “not in accordance with law.” 5 U.S.C. § 706(2)(A).

V. The Implementation Memo Exceeds DHS’s Statutory Authority (Count I).

The Implementation Memo, and the State Citizenship List regime it approves, grossly exceeds DHS’s statutory authority. 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). To determine “whether an agency has acted within its statutory authority,” courts use “the traditional tools of statutory construction.” *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 403, 412 (2024). And the APA mandates that courts “shall” set aside agency action that is “not in accordance with law” or “in excess of statutory jurisdiction, authority, or limitations.” 5 U.S.C. §§ 706(2)(A), (C).

No statute authorizes DHS to obtain hundreds of millions of U.S. citizens’ sensitive personal information from SSA, DOS, and other agencies; disclose that information in bulk to States through the Portal; and create its own “consolidated list of United States citizens” and their states of residence. *See Hill Decl. Ex. A* at 2–3. DHS insists this sprawling new regime is authorized by 8 U.S.C. § 1373, a section of the Immigration Reform and Immigrant Responsibility Act of 1996 (“1996 Act”), Pub. L. No. 104-208, 110 Stat. 3009-546. *See Hill Decl. Ex. A* at 2.⁶ But as the *LWW* court held, DHS’s reading of § 1373 is refuted by “normal rules of statutory

⁶ Although the Implementation Memo invokes, in passing, the Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359, *Hill Decl. Ex. A* at 2, the Memo itself recognizes that law only authorizes the creation of a “system for verifying the immigration status of *alien* applicants for and recipients of certain federally funded *benefits*”—not for U.S. citizens. *Id.* at 2 (emphasis added); *see* 42 U.S.C. § 1320b-7 note; *id.* § 1320b-7(d).

interpretation” and the Executive Branch’s longstanding construction of the statute. 2026 WL 1784297, at *32–33.

Start with § 1373(a). It provides that “[n]otwithstanding any other provision of Federal, State, or local law, a Federal, State, or local government entity or official may not prohibit, or in any way restrict, any government entity or official from sending to, or receiving from, [DHS] information regarding the citizenship or immigration status, lawful or unlawful, of any individual.” 8 U.S.C. § 1373(a). This provision uses purely prohibitory language, stating that government entities “*may not* prohibit, or in any way restrict” certain action. Prohibitory language such as “shall not” or “may not” is not “an affirmative grant of power.” *See New England Power Co. v. New Hampshire*, 455 U.S. 331, 341 (1982). Nothing in § 1373(a) affirmatively authorizes DHS and SSA to freely exchange data for purposes of verifying “citizen and immigration status,” notwithstanding preexisting statutory restrictions on such inter-agency disclosures. And the “Executive Branch interpretation . . . issued roughly contemporaneously with enactment of the statute” and “the longstanding ‘practice of the government’” since the 1996 Act’s enactment confirms that this is not the case. *Loper Bright*, 603 U.S. at 386; *see Relationship Between Illegal Immigr. Reform & Immigrant Resp. Act of 1996 & Statutory Requirement for Confidentiality of Census Info.*, 23 Op. O.L.C. (May 18, 1999), 1999 WL 34995963, at *4 (§ 1373(a) does “not clearly invest governmental officials or entities with the affirmative authority to disclose information in circumstances where they otherwise would be prohibited from doing so by a federal statute”). Section 1373(a) does not authorize DHS *to do* anything—it is merely a *prohibition* on conduct. *See LWV*, 2026 WL 1784297, at *33.

Nor does § 1373(c) authorize DHS’s implementation plan. That provision says DHS “shall respond to an inquiry by a Federal, State, or local government agency, seeking to verify or ascertain

the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law, by providing the requested verification or status information.” 8 U.S.C. § 1373(c). Nothing in it authorizes DHS to *obtain records* from *other* federal agencies and disclose them to States.

DHS’s contrary position that § 1373(c) empowers it to consolidate millions of U.S. citizens’ personal information stored across federal agencies and funnel it to States however it sees fit—notwithstanding the preexisting restrictions of the Social Security Act and the Privacy Act, *see supra* Argument §§ II, III—runs headlong into the “strong presumption that repeals by implication are disfavored and that Congress will specifically address preexisting law when it wishes to suspend its normal operations in a later statute.” *Epic Sys. Corp. v. Lewis*, 584 U.S. 497, 510 (2018). Indeed, nothing in § 1373(c) “expressly contradict[s]” the earlier-enacted statutes. *Nat’l Ass’n of Home Builders v. Defs. of Wildlife*, 551 U.S. 644, 662 (2007). Nor is DHS’s reading “absolutely necessary ... in order that [the] words [of the later statute] shall have any meaning at all.” *Id.* To the contrary, all statutes peacefully coexisted for 40 years until DHS concocted the State Citizenship List process in a rush to implement the President’s 2026 Elections EO. “[T]here is no reason to believe that an implied repeal or amendment of the protections of the Privacy Act or Social Security Act is ‘absolutely necessary’ for the verification provisions in Section 1373(c) to have any effect.” *LWV*, 2026 WL 1784297, at *32-33.

“Moreover, ‘the overall statutory scheme’ of the 1996 Act also does not support the Defendants’ interpretation” of § 1373. *Id.* at *33 (quoting *West Virginia v. EPA*, 597 U.S. 697, 721 (2022)). Another section of the 1996 Act, creating the E-Verify program,⁷ demonstrates “Congress knew how to” permit data sharing between DHS and SSA “when it wanted to” and that it “chose

⁷ “E-Verify is an internet-based system that allows an employer to verify an employee’s work-authorization status.” *Chamber of Com. of U.S. v. Whiting*, 563 U.S. 582, 590 (2011) (cleaned up) (discussing program).

not to in Section 1373(a) or (c).” *Id.* (quoting *Allina Health Servs. v. Price*, 863 F.3d 937, 944 (D.C. Cir. 2017) (Kavanaugh, J.)); *see* Pub. L. No. 104-208, §§ 404(e)-(f), 110 Stat. 3009, 664-65 (1996) (codified at 8 U.S.C. § 1324a note); *id.* §§ 404(e), (h) (prohibiting SSA from “disclos[ing] or releas[ing] social security information (other than such confirmation or nonconfirmation)” and from “utiliz[ing] any information, data base, or other records” in the E-Verify program “for any other purpose”). That the 1996 Act includes no similar provisions authorizing inter-agency data sharing for purposes of compiling and transmitting State Citizenship Lists (or anything like them) is a “manifestation of a considered congressional judgment.” *United States v. Fausto*, 484 U.S. 439, 448 (1988); *see also City & Cnty. of S.F. v. EPA*, 604 U.S. 334, 344 (2025) (“Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.”).

The major questions doctrine and its “clear statement” rule doubly confirm this conclusion. *See Biden v. Nebraska*, 600 U.S. 477, 505-06 (2023). In asserting the authority to create a first-of-its-kind master list of adult U.S. citizens and their states of residence, DHS has “claim[ed] to discover in . . . long-extant statute[s] ‘an unheralded power’ representing a ‘transformative expansion [of its] . . . authority’ on matters of ‘vast . . . political significance.’” *West Virginia*, 597 U.S. at 716. The “‘lack of historical precedent’” for DHS’s actions, “coupled with the breadth of authority that it now claims, is a ‘telling indication’” that the Implementation Memo “extends beyond [DHS’s] legitimate reach.” *Nat’l Fed’n of Indep. Bus. v. Dep’t of Lab.*, 595 U.S. 109, 119 (2022) (per curiam). Confirming the “political significance” of DHS’s actions, numerous bills have been introduced in Congress seeking to authorize the type of cross-agency data sharing the Implementation Memo directs for “voter verification” inquiries. *See* SAVE America Act, H.R.

7296, 119th Cong., 2d Sess. § 2(f) (2026); SAVE Act, H.R. 22, 119th Cong., 1st Sess., § 2(f) (2025); SAVE Act, H.R. 8281, 118th Cong., 2d Sess., § 2(f) (2024). None have passed the Senate, despite the Administration’s vigorous support. *See id.* Thus, DHS’s Implementation Memo “has ‘conveniently enabled it to enact a program’ that Congress has chosen not to enact itself.” *Biden*, 600 U.S. at 504. Because DHS cannot point to any “‘clear congressional authorization’ for the power it claims,” *West Virginia*, 597 U.S. at 716, 724, the major questions doctrine underscores: it has exceeded its authority.

VI. EPIC Has Standing to Challenge DHS Defendants’ Illegal Actions.

DHS’s Implementation Memo prescribes an unprecedented course of action that entails several federal agencies compiling millions of records of Americans’ sensitive personal data—using a methodology shrouded in secrecy and subject to no oversight or corrective mechanism—with plans to broadly distribute that admittedly inaccurate and incomplete information to impact voters’ access to the ballot box. This scheme has caused or will imminently cause EPIC and its members concrete injuries that confer Article III standing.

“To establish standing, a plaintiff must show: ‘(i) that [it] suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief.’” *AFSCME v. Soc. Sec. Admin.*, 172 F.4th 361, 367 (4th Cir. 2026) (en banc) (quoting *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021)). A “material risk of future harm” can constitute a cognizable injury. *TransUnion*, 594 U.S. at 435; *see also Leaders of a Beautiful Struggle v. Baltimore Police Dep’t*, 456 F. Supp. 3d 699, 710–11 (D. Md. 2021) (an individual can assert a “concrete and imminent” injury where a government agency “has clearly indicated” that it will unlawfully collect their private information), *rev’d and remanded on other grounds*, 2 F.4th 330 (4th Cir. 2021) (en banc). An organization like EPIC can assert standing both “as a representative of its members who have

been harmed” and in “its own right . . . for injury to itself.” *People for Ethical Treatment of Animals, Inc. v. Tri-State Zoological Park of W. Md., Inc.*, 843 F. App’x 493, 495 (4th Cir. 2021). EPIC readily satisfies the elements of standing, both as a representative of its injured members and in its own right as an organization.

A. EPIC has associational standing.

EPIC has associational standing because its members are suffering actual or imminent injuries closely related to harms “traditionally recognized as providing a basis for a lawsuit in American courts.” *Fernandez v. RentGrow, Inc.*, 116 F.4th 288, 296 (4th Cir. 2024). “[A]n organization can assert standing as the representative of its members if ‘(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization’s purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit.’” *W. Va. Rivers Coal., Inc. v. Chemours Co. FC, LLC*, 178 F.4th 102, 110–11 (4th Cir. 2026) (quoting *Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 600 U.S. 181, 199 (2023)). Defendants have caused or will imminently cause EPIC members to suffer at least three forms of injury pertinent to EPIC’s mission: privacy injuries, reputational injuries, and voting-related injuries.

Privacy injuries. DHS’s Implementation Memo and the course of action it prescribes have caused or will imminently cause EPIC members concrete privacy injuries that are closely analogous to the common law tort of intrusion upon seclusion, defined as the “intentional[] intru[sion], physical[] or otherwise, upon the solitude or seclusion of another or his private affairs or concerns” that “would be highly offensive to a reasonable person.” Restatement (Second) of Torts § 652B (A.L.I. 1977) (Second Restatement).

The Fourth Circuit’s recent *AFSCME* ruling expressly confirms this analogy for standing purposes. Faced with a challenge to SSA’s decision to grant DOGE access to millions of personal

records, the *en banc* court concluded that SSA’s wrongful disclosure of personal data—even to another federal entity—“inflict[ed] a harm that is a ‘close . . . analogue’ to the common law tort of intrusion upon seclusion,” *AFSCME*, 172 F.4th at 368, and thus worked an injury in fact. Here, EPIC members are suffering injuries nearly identical to those in *AFSCME*: Defendants have or imminently will impermissibly aggregate, misuse, and divulge the Social Security numbers and citizenship data of EPIC members without their consent to other entities. *See* Kisselburgh Decl. ¶¶ 18-25; Nel Decl. ¶¶ 39–43; *supra* Argument § I. These statutory violations parallel both essential features of intrusion upon seclusion: (1) an intentional intrusion into private affairs, which (2) would be “highly offensive to a reasonable person.” *AFSCME*, 172 F.4th at 369 (quoting Restatement (Second) of Torts § 652B); *see also* Kisselburgh Decl. ¶¶ 18-25; Nel Decl. ¶ 39–43. EPIC members confirm that these disclosures are highly offensive to them. Kisselburgh Decl. ¶ 21; Nel Decl. ¶¶ 43, 49. Their privacy injuries, like those in *AFSCME*, are thus concrete and cognizable.

Defendants’ conduct also works a concrete privacy injury closely analogous to a breach of confidence. “That tort ‘lies where a person offers private information to a third party in confidence and the third party reveals that information to another.’” *AFSCME v. Soc. Sec. Admin.*, No. 25-1411, 2025 WL 1249608, at *44 n.33 (4th Cir. Apr. 30, 2025) (King, J., concurring) (quoting *AFL-CIO v. Dep’t of Lab.*, 778 F. Supp. 3d 56, 73 (D.D.C. 2025)). EPIC members provided their citizenship and other information to SSA in confidence when they applied for SSNs and reasonably expected it to be kept confidential based on longstanding statutory protections and agency policies. Kisselburgh Decl. ¶ 18; Nel Decl. ¶ 39. And EPIC members reasonably expected that DHS and other federal agencies would maintain the confidentiality of the personal information entrusted to them, consistent with the strictures of the Privacy Act. Kisselburgh Decl. ¶¶ 18-20; Nel Decl.

¶¶ 39–42. Indeed, “[f]or decades,” SSA has “guarded” Americans’ “sensitive” “data scrupulously, and Americans trusted it to do so.” *AFSCME*, 172 F.4th at 365. To this day, SSA policy assures the public 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.” Hill Decl. Ex. V at 6. Defendants’ betrayal of trust in consolidating, misusing, and disclosing EPIC members’ sensitive personal information closely tracks the type of injury vindicated by the tort of breach of confidence. *See Jeffries v. Volume Servs. Am.*, 928 F.3d 1059, 1064 (D.C. Cir. 2019).

Reputational injuries. Defendants’ statutory violations have inflicted or will imminently inflict harms on EPIC members similar to those vindicable through the common law tort of defamation. Defendants have adopted an unlawful policy of disclosing citizenship information that is derived in significant part from SSA records, which the agencies themselves concede are incomplete and unfit for verifying citizenship. *See* Hill Decl. Exs. A, N, O. Defendants’ reliance on this erroneous data makes it highly likely that many derived and naturalized citizens—including EPIC member Anthony Nel, a derived citizen—will be erroneously omitted from or miscategorized in the State Citizenship Lists and related data disclosed by DHS. Nel Decl. ¶¶ 40, 43–47. Indeed, in 2025, Nel was misidentified as a non-citizen and had his voter registration cancelled due to Texas’s use of the modified SAVE system, which relies on the same faulty SSA citizenship data DHS is incorporating into its State Citizenship Lists. Nel Decl. ¶¶ 35, 37, 39–40. And he remains at high risk of being falsely characterized as a non-citizen, despite being a lawfully registered voter. Nel Decl. ¶¶ 40, 43–47. The injury associated with such false statements bears a “close relationship” to the reputational harm associated with the tort of defamation. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 432 (2021). In *Transunion*, the defendant provided third parties

with information labeling the plaintiff class members as potential criminals. *Id.* So too here: It is a federal crime for non-citizens to vote or register to vote in federal elections. *See* 18 U.S.C. §§ 611, 1015(f). For Defendants to produce State Citizenship Lists and other citizenship data implicitly or explicitly designating Nel as a non-citizen therefore works a harm closely analogous to defamation, and by extension a concrete reputational injury. *See LWV*, 2026 WL 1784297, at *12 (individuals misidentified as non-citizens by SAVE suffered reputational injury).

Voting-related injuries. Defendants’ unlawful policy of consolidating, misusing, and disclosing citizenship data has caused or will imminently cause injury to EPIC members’ voting rights. “[V]oters who allege facts showing disadvantage to themselves as individuals have standing to sue to remedy that disadvantage.” *Maryland Election Integrity, LLC v. Maryland State Bd. of Elections*, 127 F.4th 534, 539 (4th Cir. 2025) (quoting *Gill v. Whitford*, 585 U.S. 48, 65–66 (2018)) (cleaned up). A voter “need not have the franchise wholly denied to suffer injury.” *Charles H. Wesley Educ. Found., Inc. v. Cox*, 408 F.3d 1349, 1352 (11th Cir. 2005). Rather, “any concrete, particularized, non-hypothetical” burden on the right to vote “is sufficient.” *Id.* For example, “[c]oncerns about the security and privacy of an applicant’s full SSN” can both impose a “substantial burden” on the right to vote, *Democratic Party of Virginia v. Brink*, 599 F. Supp. 3d 346, 360 (E.D. Va. 2022) (citing *Greidinger v. Davis*, 988 F.2d 1344, 1348 (4th Cir. 1993)), and support an injury in fact sufficient for standing, *id.* at 354–56.

Certain EPIC members face an elevated risk of being erroneously removed from the voter rolls due to Defendants’ actions, which cognizably threatens burdening those members’ right to vote. For the same reasons Nel and similarly situated members have suffered or will imminently suffer a reputational injury, they face a high risk of being erroneously deregistered and disenfranchised because of Defendants’ reliance on erroneous SSA records to assemble the

citizenship data and construct the State Citizenship Lists. Nel Decl. ¶¶ 43–47. Being misidentified as a non-citizen and deregistered on that basis would at minimum force those EPIC members to provide documented proof of citizenship to restore their registrations, Nel Decl. ¶¶ 45–46, and could also cause outright disenfranchisement. This burden on the right to vote constitutes a “concrete, particularized, non-hypothetical” injury in fact, *Charles H. Wesley Educ. Found.*, 408 F.3d at 1352; *see also Mi Familia Vota v. Fontes*, 129 F.4th 691, 708–09 (9th Cir. 2025).

EPIC meets the other elements of associational standing. EPIC is seeking to protect the rights of its members in furtherance of its “mission [] to secure the fundamental right to privacy in the digital age.” Butler Decl. ¶ 3. And EPIC members’ “individual participation” is not “necessary” because EPIC “seeks prospective or injunctive relief for its members[.]” *United Food & Com. Workers Union Loc. 751 v. Brown Grp., Inc.*, 517 U.S. 544, 546 (1996).

B. EPIC has informational standing.

Defendants’ failure to make statutorily required public disclosures about their compilation and distribution of citizenship data has inflicted or will imminently inflict a concrete informational injury on EPIC by impairing the organization’s ability to perform mission-critical functions. To establish standing based on an informational injury, an organization “must demonstrate that it suffered ‘a real harm with an adverse effect’ resulting from the failure to receive” information to which it is legally entitled, *Pub. Int. Legal Found., Inc. v. Wooten*, 164 F.4th 362, 366 (4th Cir. 2026), and that it “suffers, by being denied access to that information, the type of harm Congress sought to prevent by requiring disclosure,” *Dreher v. Experian Info. Sols., Inc.*, 856 F.3d 337, 345–46 (4th Cir. 2017).

EPIC has long relied extensively on information that the Privacy Act requires agencies to disclose, including information in SORNs. Butler Decl. ¶¶ 8–11. 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, how that information may be used and disclosed, what burdens collection will impose, how it will be stored and secured, and for how long it will be retained. Butler Decl. ¶ 12; *see also* 5 U.S.C. § 552a(e)(4). 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, and to craft targeted Freedom of Information Act requests for agency records. Butler Decl. ¶¶ 8-11.

By unlawfully withholding required information from the public, Defendants have harmed or will imminently harm EPIC by directly preventing it from “effectively carrying out its mission” and “evaluat[ing]” matters of public concern core to its operations. *National Veterans Legal Servs. Program v. U.S. Department of Defense*, 990 F.3d 834, 838 (4th Cir. 2021). Denial of statutorily required information that interferes with an organization’s mission-critical functions is “just the kind of injury found to have established standing in” *Federal Election Commission v. Akins*, 524 U.S. 11 (1998). *NVLSP v. U.S. Dep’t of Def.*, 990 F.3d 834, 838 (4th Cir. 2021). “So it is here,” *NVLSP*, 990 F.3d at 838, where EPIC has been denied essential information from the absent SORNs that it would otherwise rely upon to educate its members, voters, the press, and the public at large about the risks posed by the government’s compilation and distribution of citizenship data and how to mitigate them—all of which are mission-critical functions of EPIC. Butler Decl. ¶¶ 15-18.

C. EPIC and its members have procedural standing.

EPIC has procedural standing because Defendants’ violations of the Privacy Act’s notice-and-comment requirements impair the above-described “concrete interest[s]” that the Act “was designed to protect.” *Hodges v. Abraham*, 300 F.3d 432, 445 (4th Cir. 2002); *see also LWV*, 2026 WL 1784297, at *18–19. By failing to publish applicable SORNs and solicit public comment on them as Act requires, Defendants have committed procedural violations that deny EPIC its rightful

opportunity to participate, impede EPIC’s core interests in transparency and public education about personal data collection, and hamper EPIC’s ability to carry out its mission. Butler Decl. ¶¶ 19-21. The same procedural violations frustrate the concrete interests of EPIC members, many of whom have submitted comments and provided testimony to the government on privacy matters and would have liked to provide comments on Defendants’ compilation and transmission of State Citizenship Lists in defense of their privacy, reputations, and voting rights. Butler Decl. ¶ 11; Kisselburgh Decl. ¶ 7.

D. The other elements of standing are satisfied.

The injuries to EPIC and its members are all traceable to Defendants’ unlawful policy of consolidating, misusing, and disclosing citizenship data and their failure to comply with required procedures. But for the DHS Implementation Memo and its prescribed “course of action,” Implementation Memo at 1, none of EPIC’s injuries would occur. “Because Article III ‘requires no more than de facto causality,’ traceability is satisfied here.” *Dep’t of Com. v. New York*, 588 U.S. 752, 768 (2019) (citation modified) (citing cases). Redressability is also easily met. Plaintiff’s requested relief would redress their injuries by requiring Defendants to vacate DHS’s Implementation Memo, to undo the memo’s effects, and to publish applicable SORNs to the extent that Defendants still seek to proceed.

VII. Plaintiff Is Entitled to its Requested Relief.

A. The Court should set aside the Implementation Memo and associated actions.

The APA mandates that “a ‘reviewing court shall . . . hold unlawful and set aside agency action” that is in excess of statutory authority, contrary to law, or procedurally defective. 5 U.S.C. § 706(2)(A)–(D). Here, if the Court finds that Plaintiff has prevailed on any of the APA claims relevant to this motion (Counts I-IV), the Court is “bound” to apply this rule and set aside the unlawful action. *Friends of Back Bay v. U.S. Army Corps of Eng’rs*, 681 F.3d 581, 586–87 (4th Cir.

2012). Indeed, “[v]acatur is the normal remedy under the APA.” *Sierra Club v. Nat’l Marine Fisheries Serv.*, 797 F. Supp. 3d 440, 493 (D. Md. 2024). “Vacatur of agency action is commonly understood to mean restoration of the status quo.” *Child Trends, Inc. v. U.S. Dep’t of Educ.*, 795 F. Supp. 3d 700, 731 (D. Md. 2025). Here, vacatur of the Implementation Memo requires DHS Defendants to cease all actions taken pursuant to the Memo including dismantling the Portal; disgorging and unlinking all associated data; and withdrawing all associated policies and agreements. Such relief is necessary to “restor[e] ... the status quo,” *id.*, as if the “disapproved agency action ... never happened,” *Griffin*, 144 S. Ct. at 2 n.1 (Kavanaugh, J., concurring).

B. In the alternative, the Court should issue a permanent injunction.

In the alternative, should the Court find vacatur alone does not encompass Plaintiff’s requested relief (notwithstanding Plaintiff’s position outlined *supra*), the APA further authorizes the Court to issue “writs of prohibitory or mandatory injunction.” 5 U.S.C. § 703; *see also Doe*, 435 F.3d at 505 (APA authorizes injunctive relief for Privacy Act violations). Thus, Plaintiff alternatively requests that the Court permanently enjoin the Implementation Memo and actions by DHS Defendants and those acting in concert with them taken pursuant to it, including but not limited to the creation and disclosure of the State Citizenship Lists and the Portal.⁸ *See* Fed. R. Civ. P. 65(d)(2). Such a remedy is warranted here because, as discussed *supra* Argument § IV Plaintiff’s and its members’ injuries stem from the misappropriation of sensitive personal information in violation of statute. In these circumstances, a court can remedy the injury resulting

⁸ Defendants’ actions will “irreparably harm Plaintiff[’s] interests in the absence of an injunction because, in the inherently time-constrained context of an election cycle, the Court cannot provide meaningful redress for lost opportunities[.]” *LULAC*, 818 F. Supp. 3d at 102. And, unauthorized disclosure of highly sensitive personal information “is a bell that one cannot unring.” *Senior Executives Ass’n v. United States*, 891 F. Supp. 2d 745, 755 (D. Md. 2012); *see also supra* Argument § III.A. EPIC is losing the opportunity to use its limited resources to educate and protect the privacy of its members and the general public in furtherance of its mission. *See supra* Argument §§ III.B, C. Because “agencies have no legitimate interest in the perpetuation of unlawful practices” and “the public interest ‘favors permitting as many qualified voters to vote as possible,’” the “balance of hardships and the public interest weigh in favor of granting a permanent injunction.” *LULAC*, 818 F. Supp. 3d at 91 (quoting *Newby*, 838 F.3d at 12).

from “the Government’s continued possession of those materials” by ordering “the Government to destroy . . . any and all copies it may have in its possession.” *Church of Scientology of Cal. v. United States*, 506 U.S. 9, 13 (1992); *accord AFSCME*, 172 F.4th at 373; *Chastain v. Kelley*, 510 F.2d 1232, 1235 (D.C. Cir. 1975).

C. The Court should declare the Defendants’ challenged actions unlawful.

A declaratory judgment is also warranted because “the judgment will serve a useful purpose in clarifying and settling the legal relations in issue, and when it will terminate and afford relief from the uncertainty, insecurity, and controversy giving rise to the proceeding.” *Penn-Am. Ins. Co. v. Coffey*, 368 F.3d 409, 412 (4th Cir. 2004) (cleaned up); *see also LULAC*, 818 F. Supp. 3d at 90–91. Declaring the challenged actions unlawful will clarify and settle issues of unquestionable public importance and uncertainty, particularly given the looming nationwide midterm elections, imminent disclosure of highly sensitive information pursuant to the deadlines in the Implementation Memo, and depth and breadth of the privacy violations.

CONCLUSION

Plaintiff requests that the Court grant Plaintiff’s motion for partial summary judgment.

Dated: September 3, 2026

Respectfully submitted,

R. Orion Danjuma*
Julia L. Torti*
PROTECT DEMOCRACY PROJECT

[REDACTED]

Sara Chimene-Weiss*
PROTECT DEMOCRACY PROJECT

[REDACTED]

Jane Bentrrott*
Shelby Teeter*
PROTECT DEMOCRACY PROJECT

[REDACTED]

/s/ Nikhel S. Sus
Nikhel S. Sus (Bar No. 31090)
John B. Hill**
Reuven Dashevsky**
CITIZENS FOR RESPONSIBILITY
AND ETHICS IN WASHINGTON

[REDACTED]

John Davisson*
Mayu Tobin-Miyaji*
ELECTRONIC PRIVACY INFORMATION CENTER

[REDACTED]

Counsel for Plaintiff

* *Pro hac vice* motion forthcoming

** *Pro hac vice* motion filed