

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*

Defendants.

Case No. 1:26-cv-01352-SLS

PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

Pursuant to Federal Rule of Civil Procedure 56 and Local Civil Rule 7(h), Plaintiffs Anthony Nel, Haley Smith, Linda Duckworth, Ruth Nasrullah, Common Cause, and Common Cause Education Fund respectfully move for summary judgment on Counts I, VI, VII, and VIII of Plaintiffs' Complaint (ECF No. 1). For the reasons set forth in the accompanying Memorandum of Law, Plaintiffs are entitled to summary judgment on Counts I, VI, VII, and VIII of their Complaint. In support of this Motion, Plaintiffs submit the attached Declarations of John B. Hill (Exhibit A), Elena Nunez (Exhibit B), Gavin Geis (Exhibit C), Julia Vaughn (Exhibit D), Catherine Turcer (Exhibit E), Anthony Gutierrez (Exhibit F), Plaintiff Anthony Nel (Exhibit G), Plaintiff Linda Duckworth (Exhibit H), Plaintiff Ruth Nasrullah (Exhibit I), Plaintiff Haley Smith (Exhibit J), Alex Doe (Exhibit K), Bailey Doe (Exhibit L), Claudio Mosse (Exhibit M), and Mohammed Nasrullah (Exhibit N). A proposed order is also attached.

Plaintiffs request an oral hearing on this motion pursuant to Local Civil Rule 7(f).

Dated: May 19, 2026

Respectfully submitted,

By: /s/ Nikhel S. Sus

Nikhel S. Sus (D.C. Bar No. 1017937)
John B. Hill (N.Y. Bar No. 5505508)*
CITIZENS FOR RESPONSIBILITY
AND ETHICS IN WASHINGTON
P.O. Box 14596 Washington, DC 20044
Tel: (202) 408-5565
nsus@citizensforethics.org
jhill@citizensforethics.org

Sara Chimene-Weiss*
PROTECT DEMOCRACY PROJECT
7000 N. 16th Street, Suite 120, #340
Phoenix, AZ 85020
Tel: (202) 934-4237
sara.chimene-weiss@protectdemocracy.org

Jane Bentrott (D.C. Bar No. 1029681)
Naomi Gilens (D.C. Bar No. 90037831)
PROTECT DEMOCRACY PROJECT
2020 Pennsylvania Ave. NW, Suite # 163
Washington DC 20006
Tel: (202) 579-4582
Fax: (202) 769-3176
jane.bentrott@protectdemocracy.org
naomi.gilens@protectdemocracy.org

Jared Fletcher Davidson*
PROTECT DEMOCRACY PROJECT
82 Nassau St., #601
New York, NY 10038
Tel: (202) 579-4582
jared.davidson@protectdemocracy.org

John Haubenreich*
PROTECT DEMOCRACY PROJECT
1108 McKennie Ave., Suite #223
Nashville, TN 37206
Tel: (202) 579-4582
john.haubenreich@protectdemocracy.org

Laurence M. Schwartztol (D.D.C. Bar No. MA0007)
DEMOCRACY AND RULE OF LAW CLINIC,

HARVARD LAW SCHOOL
1525 Massachusetts Avenue
Cambridge, MA 02138
Tel: (617) 998-1877
lschwartztol@law.harvard.edu

Ming Cheung*
Ari J. Savitzky*
Theresa J. Lee*
Sophia Lin Lakin*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Tel: (212) 549-2500
mcheung@aclu.org
asavitzky@aclu.org
tlee@aclu.org
slakin@aclu.org

Laura K. Follansbee (D.C. Bar No. 1782046)
Arthur B. Spitzer (D.C. Bar No. 235960)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF THE DISTRICT OF COLUMBIA
529 14th Street NW, Suite 722
Washington, DC 20045
Tel: (202) 457-0800
lfollansbee@acludc.org
aspitzer@acludc.org

* Admitted *pro hac vice*

Counsel for Plaintiffs

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

**MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS'
MOTION FOR PARTIAL SUMMARY JUDGMENT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTRODUCTION 1

BACKGROUND 3

 I. DOJ’s Voter List Maintenance Policy 3

 A. President Trump’s efforts to “nationalize” elections and DOJ’s Voter List Maintenance Policy..... 3

 B. Compiling state voter registration lists 5

 C. Disclosing SVRLs to DHS and external third parties..... 7

 D. Using DHS’s error-riddled SAVE system to check voter eligibility 8

 E. Directing states to remove voters..... 10

 F. The Administrative Record..... 11

 II. Impact of DOJ’s Voter List Maintenance Policy on the Plaintiffs 11

LEGAL STANDARD..... 12

ARGUMENT 12

 I. Plaintiffs have standing..... 12

 II. Plaintiffs challenge final agency action 19

 III. Plaintiffs are entitled to summary judgment on Counts I, VI, VII, and VIII of the Complaint..... 20

 A. DOJ’s Voter List Maintenance Policy lacks statutory authorization (Count I) 20

 B. DOJ’s Voter List Maintenance Policy violates the Privacy Act (Count VI) 25

 1. DOJ violated the Privacy Act’s notice-and-comment requirements for revising systems of records 25

 2. DOJ is improperly disclosing records in bulk in violation of the Privacy Act 28

 3. DOJ is maintaining inaccurate and outdated records in bulk in violation of the Privacy Act..... 30

 4. DOJ is maintaining First Amendment protected records in bulk in violation of the Privacy Act 32

 C. DOJ’s Voter List Maintenance Policy violates the Paperwork Reduction Act (Count VII)..... 34

 D. DOJ’s Policy is arbitrary and capricious (Count VIII) 37

 1. Defendants failed to explain the Policy 38

 2. DOJ failed to explain a rational connection between the facts and the Policy 38

3.	DOJ entirely failed to consider important aspects of the problem.....	39
IV.	Plaintiffs are entitled to their requested relief.....	42
A.	The Court should set aside and vacate the Policy under the APA.....	42
B.	Alternatively, the Court should permanently enjoin the Voter List Maintenance Policy	43
C.	The Court should declare the Policy unlawful.....	45
	CONCLUSION.....	45

TABLE OF AUTHORITIES

Cases

<i>AFL-CIO v. Dep’t of Lab.</i> , 778 F. Supp. 3d 56 (D.D.C. 2025)	17, 25
<i>AFSCME v. SSA</i> , 172 F.4th 361 (4th Cir. 2026) (en banc)	16, 44
<i>Ala. Ass’n of Realtors v. HHS</i> , 594 U.S. 758 (2021)	21
<i>Allina Health Servs. v. Sebelius</i> , 746 F.3d 1102 (D.C. Cir. 2014)	42
<i>Am. Bioscience, Inc. v. Thompson</i> , 269 F.3d 1077 (D.C. Cir. 2001)	12
<i>Am. Civ. Rts. Union v. Phila. City Comm’rs</i> , 872 F.3d 175 (3d Cir. 2017)	22
<i>Am. Fed’n of Tchrs. v. Dep’t of Educ.</i> , 796 F. Supp. 3d 66 (D. Md. 2025)	39
<i>Amerijet Int’l, Inc. v. Pistole</i> , 753 F.3d 1343 (D.C. Cir. 2014)	38
<i>Ames v. DHS</i> , 861 F.3d 238 (D.C. Cir. 2017)	29
<i>Amfac Resorts v. U.S. Dep’t of the Interior</i> , 143 F. Supp. 2d 7 (D.D.C. 2001)	37
<i>Bellitto v. Snipes</i> , 935 F.3d 1192 (11th Cir. 2019)	22
<i>Bennett v. Spear</i> , 520 U.S. 154 (1997)	19
<i>Bhd. of Locomotive Eng’rs & Trainmen v. Fed. R.R. Admin.</i> , 972 F.3d 83 (D.C. Cir. 2020)	37
<i>Bldg. Trades Unions v. Dep’t of Def.</i> , 783 F. Supp. 3d 290 (D.D.C. 2025)	43
<i>Brakebill v. Jaeger</i> , 905 F.3d 553 (8th Cir. 2018)	5
<i>Bridgeport Hosp. v. Becerra</i> , 108 F.4th 882 (D.C. Cir. 2024)	42
<i>California v. Trump</i> , 786 F. Supp. 3d 359 (D. Mass. 2025)	4
<i>Carlson v. Postal Regul. Comm’n</i> , 938 F.3d 337 (D.C. Cir. 2019)	42
<i>Chapman v. Hou. Welfare Rts. Org.</i> , 441 U.S. 600 (1979)	21

Cases—Cont.

<i>Chastain v. Kelley</i> , 510 F.2d 1232 (D.C. Cir. 1975).....	44
<i>Chichakli v. Tillerson</i> , 882 F.3d 229 (D.C. Cir. 2018).....	28
<i>Church of Scientology of Cal. v. United States</i> , 506 U.S. 9 (1992).....	44
<i>City of Billings v. TSA</i> , 153 F.4th 46 (D.C. Cir. 2025).....	43
<i>Council of Parent Att’ys & Advocs., Inc. v. DeVos</i> , 365 F. Supp. 3d 28 (D.D.C. 2019).....	40
<i>CREW v. DOJ</i> , 2026 WL 472589 (D.D.C. Feb. 19, 2026).....	16
<i>Ctr. for Biological Diversity v. Dep’t of Interior</i> , 144 F.4th 296 (D.C. Cir. 2025).....	12
<i>Ctr. for Biological Diversity v. U.S. Int’l Dev. Fin. Corp.</i> , 77 F.4th 679 (D.C. Cir. 2023).....	15
<i>Daimler Trucks N. Am. LLC v. EPA</i> , 737 F.3d 95 (D.C. Cir. 2013).....	43
<i>Dep’t of Com. v. New York</i> , 588 U.S. 752 (2019).....	19, 38
<i>Diamond Alt. Energy, LLC v. EPA</i> , 606 U.S. 100 (2025).....	19
<i>Doctors for America v. OPM</i> , 766 F. Supp. 3d 39 (D.D.C. 2025).....	34
<i>Dole v. United Steelworkers of Am.</i> , 494 U.S. 26 (1990).....	36
<i>Drs. for Am. v. OPM</i> , 793 F. Supp. 3d 112 (D.D.C. 2025).....	21
<i>FCC v. Fox Television Stations, Inc.</i> , 556 U.S. 502 (2009).....	38, 41
<i>FDA v. All. for Hippocratic Med.</i> , 602 U.S. 367 (2024).....	13
<i>FEC v. Cruz</i> , 596 U.S. 289 (2022).....	21
<i>Friends of the Earth, Inc. v. Laidlaw Env’t Servs. (TOC), Inc.</i> , 528 U.S. 167 (2000).....	12
<i>Gerlich v. DOJ</i> , 711 F.3d 161 (D.C. Cir. 2013).....	33
<i>Hyatt v. OMB</i> , 908 F.3d 1165 (9th. Cir. 2018).....	34, 35

Cases—Cont.

<i>Indep. Mkt. Monitor for PJM v. FERC</i> , 162 F.4th 1167 (D.C. Cir. 2025).....	15
<i>Las Ams. Immigrant Advoc. Ctr. v. DHS</i> , 783 F. Supp. 200 (D.D.C. 2025).....	42, 43
<i>League of United Latin Am. Citizens (“LULAC I”) v. EOP</i> , 808 F. Supp. 3d 29 (D.D.C. Oct. 31, 2025)	4, 21, 45
<i>League of United Latin Am. Citizens (“LULAC II”) v. EOP</i> , 818 F. Supp. 3d 34 (D.D.C. Jan. 30, 2026).....	4, 17, 21, 25, 28, 41, 44, 45
<i>League of Women Voters of U.S. v. Newby</i> , 838 F.3d 1 (D.C. Cir. 2016).....	13, 15, 44, 45
<i>League of Women Voters v. DHS</i> , 2025 WL 3198960 (D.D.C. Nov. 17, 2025)	32
<i>MacPherson v. IRS</i> , 803 F.2d 479 (9th Cir. 1986)	34
<i>Marin Audubon Soc’y v. FAA</i> , 121 F.4th 902 (D.C. Cir. 2024).....	21
<i>Massachusetts v. Dep’t of Educ.</i> , 2026 WL 918941 (D. Mass. Apr. 3, 2026).....	43
<i>Massachusetts v. EPA</i> , 549 U.S. 497 (2007).....	19
<i>Maydak v. United States</i> , 363 F.3d 512 (D.C. Cir. 2004).....	34
<i>Mendoza v. Perez</i> , 754 F.3d 1002 (D.C. Cir. 2014).....	19
<i>Mi Familia Vota v. Fontes</i> , 129 F.4th 691 (9th Cir. 2025)	17
<i>Motor Vehicle Mfrs. Ass’n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.</i> , 463 U.S. 29 (1983).....	37, 39
<i>Nat’l Ass’n of Home Builders v. Norton</i> , 298 F. Supp. 2d 68 (D.D.C. 2003).....	20
<i>Nat’l Fed’n of Indep. Bus. v. Dep’t of Lab.</i> , 595 U.S. 109 (2022) (per curiam).....	25
<i>Nat’l Lifeline Ass’n v. Fed. Commc’ns Comm’n</i> , 921 F.3d 1102 (D.C. Cir. 2019)	38, 39, 40
<i>Orr v. Trump</i> , 778 F. Supp. 3d 394 (D. Mass. 2025).....	34
<i>Purcell v. Gonzalez</i> , 549 U.S. 1, (2006).....	45
<i>President v. Vance</i> , 627 F.3d 353 (D.C. Cir. 1980).....	45

Cases—Cont.

Pub. Citizen v. Fed. Motor Carrier Safety Admin.,
374 F.3d 1209 (D.C. Cir. 2004).....40

Pub. Emps. for Env’t Resp. v. Hopper,
827 F.3d 1077 (D.C. Cir. 2016).....42

Pub. Int. Legal Found., Inc. v. Nago,
2026 WL 1144703 (9th Cir. Apr. 28, 2026)22

Richardson v. Trump,
496 F. Supp. 3d 165 (D.D.C. 2020).....18

Roudebush v. Hartke,
405 U.S. 15 (1972).....21

Sandusky Cnty. Democratic Party v. Blackwell,
387 F.3d 565 (6th Cir. 2004)22

Sierra Club v. Dep’t of Transp.,
125 F.4th 1170 (D.C. Cir. 2025).....42

Sierra Club v. Salazar,
177 F. Supp. 3d 512 (D.D.C. 2016).....42

Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.,
600 U.S. 181 (2023).....16

Stuttering Found. of Am. v. Springer,
498 F. Supp. 2d 203 (D.D.C. 2007).....12

U.S. Sugar Corp. v. EPA,
113 F.4th 984 (D.C. Cir. 2024).....21

United States v. Amore,
2026 WL 1040637 (D.R.I. Apr. 17, 2026).....3, 23

United States v. Benson,
2026 WL 362789 (W.D. Mich. Feb. 10, 2026).....3

United States v. Fontes,
2026 WL 1177244 (D. Ariz. Apr. 28, 2026)3

United States v. Galvin,
2026 WL 972129 (D. Mass. Apr. 9, 2026)3, 23

United States v. Oregon,
2026 WL 318402 (D. Or. Feb. 5, 2026).....3

United States v. Weber,
816 F. Supp. 3d 1168 (C.D. Cal. Jan. 15, 2026).....3, 7, 24, 25, 27, 28, 33, 34

United to Protect Democracy v. Presidential Advisory Comm’n on Election Integrity,
288 F. Supp. 3d 99 (D.D.C. 2017).....16

Venetian Casino Resort, LLC v. EEOC,
530 F.3d 925 (D.C. Cir. 2008).....19

Washington v. Trump,
2026 WL 73866 (W.D. Wash. Jan. 9, 2026).....4

Cases—Cont.

West Virginia v. EPA,
597 U.S. 697 (2022).....21, 24

Statutes & Regulations

5 U.S.C.

§ 552a(a)(3).....31, 33
 § 552a(b)28, 30
 § 552a(b)(3)28
 § 552a(b)(7)29, 30
 § 552a(e)(4).....26, 29
 § 552a(e)(5).....31, 32, 39, 40
 § 552a(e)(6).....31, 32
 § 552a(e)(7).....33, 34
 § 552a(e)(10).....31, 32
 § 552a(e)(11).....26
 § 703.....43
 § 706(2)(A)28, 32, 37
 § 706(2)(D)26, 32, 37, 42

18 U.S.C.

§ 611(a)30
 § 1015(f).....30

42 U.S.C.

§ 1320b-7(d).....8
 § 1320b-7 note8

44 U.S.C.

§ 3501(8)(A)36
 § 3502(3)(A)35, 36
 § 3502(10).....35, 36
 § 3506(c)(1)35
 § 3506(c)(1)(B)(iii)35
 § 3506(c)(2)35
 § 3507(a)(1)35
 § 3507(a)(1)(D).....35
 § 3507(a)(2)-(3)35
 § 3508.....35
 § 3518(c)(1)37
 § 3518(c)(2)37

Statutes & Regulations—Cont.

52 U.S.C.

§ 20501(b).....	24
§ 20507.....	24
§ 20507(a)(4)	20, 21, 22
§ 20507(d)(1)(B).....	24
§ 20510(a).....	22
§ 20511.....	22
§ 21083(a)(1)(A).....	22, 23
§ 21083(a)(4)(A).....	20, 22
§ 21111.....	22
§ 21144.....	22

Immigration Reform Control Act of 1986, Pub. L. No. 99-603, title I, §121(c)(1),
100 Stat. 3359, 3391 (1986).....8

Other Authorities and Materials

<i>Acquired Citizenship</i> , USCIS Glossary of Terms.....	9
<i>Derivative Citizenship</i> , USCIS Glossary of Terms.....	9
DOJ Civil Rights Division, <i>About The National Voter Registration Act</i>	41
Exec. Order No. 14248, <i>Preserving and Protecting the Integrity of American Elections</i> , 90 Fed. Reg. 14005 (Mar. 25, 2025).....	4
Exec. Order No. 14399, <i>Ensuring Citizenship Verification and Integrity in Federal Elections</i> , 91 Fed. Reg. 17125 (Mar. 31, 2026)	4
68 Fed. Reg. 47610 (Aug. 11, 2003).....	27
70 Fed. Reg. 43904 (July 29, 2005).....	27
82 Fed. Reg. 24147 (May 25, 2017).....	27
DHS, System of Records Notice, 90 Fed. Reg. 48948 (Oct. 31, 2025).....	7
Jen Fifield & Zach Despart, “ <i>Not Ready for Prime Time.</i> ” <i>A Federal Tool to Check Voter Citizenship Keeps Making Mistakes</i> , ProPublica & Texas Tribune (Feb. 13, 2026).....	10
OMB Circular No. A-108, <i>Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act</i> , (2016)	26, 29
OMB Privacy Act Guidelines, 40 Fed. Reg. 28948 (July 9, 1975)	28
S. Rep. No. 93-1183 (1974).....	30

INTRODUCTION

In service of the President’s unlawful attempts to seize control of elections from the states, the Department of Justice (“DOJ”) has issued an unprecedented demand to every state: hand over your unredacted voter registration lists and cede to DOJ the authority to determine which voters are eligible to remain on your rolls. To effectuate this new Voter List Maintenance Policy,¹ DOJ is collecting, stockpiling in a centralized system of records, manipulating, and sharing millions of Americans’ sensitive personal data without their consent, including their Social Security numbers, driver’s license numbers, dates of birth, home addresses, voting history, and party affiliation. And DOJ is funneling entire state voter files to the Department of Homeland Security (“DHS”) to run mass citizenship checks using DHS’s unreliable Systematic Alien Verification for Entitlements (“SAVE”) system, which DHS itself admits is error-prone and likely to wrongly ensnare eligible voters. DOJ intends to then transmit the results of this flawed process back to the states with instructions to purge voters it has unilaterally deemed ineligible.

No statute authorizes DOJ’s sweeping new Policy. And the Policy affirmatively violates federal privacy laws and the bedrock requirement of the Administrative Procedure Act (“APA”) that federal agencies engage in reasoned, transparent decision making. DOJ instead adopted the Policy “discreetly” and “outside of the view of the public,” CRT-3384, without following statutory notice-and-comment procedures, studying the Policy’s risks, explaining its reasoning, or even memorializing the decision itself. The upshot of DOJ’s unlawful and unreasoned Policy is to

¹ Plaintiffs’ Complaint referred to DOJ’s “Voter Registration Nationalization Policy.” But documents in the Administrative Record refer to this policy as the “NVRA 2025 *Voter List Maintenance Project*,” “the *list maintenance project*,” and “the NVRA *List Maintenance Project*.” See, e.g., CRT-0007 (emphasis added); CRT-3387 (emphasis added); CRT-3397 (emphasis added). Accordingly, Plaintiffs will use DOJ’s terminology in referring to the Policy as the “Voter List Maintenance Policy.”

substantially threaten the privacy, security, and voting rights of millions of lawfully registered American voters. This Court must intervene.

DOJ's Policy inverts the constitutional and statutory design of American elections. The Constitution entrusts the states and Congress, not the President or his appointees, with powers over election administration. Consistent with this constitutional design, Congress has enacted carefully tailored statutes—such as the National Voter Registration Act (“NVRA”) and the Help America Vote Act (“HAVA”)—to establish uniform minimum standards for voter registration while explicitly giving each individual state discretion to implement the laws and conduct list maintenance for itself. Nowhere in these statutes, or any federal law, has Congress authorized the Executive Branch to commandeer state voter rolls and choose who is eligible to vote.

Because the Administrative Record (“AR”) lays bare the many ways that DOJ's Voter List Maintenance Policy violates federal statutes, Plaintiffs move for summary judgment on Counts I, VI, VII, and VIII of their Complaint.² First, the AR makes clear that DOJ lacks any legal authority for the Policy. Second, the Privacy Act—passed in response to the Nixon Administration's abuses of executive power—prohibits DOJ from implementing the Policy by secretly creating a centralized record system of Americans' personal data, and widely disclosing data from that system, without a necessary and lawful purpose. Third, the Paperwork Reduction Act (“PRA”) requires additional safeguards before an agency may collect personal information, which DOJ has openly defied here. Finally, having submitted a threadbare AR composed entirely of post-hoc

² Counts II-V assert that DOJ's Voter List Maintenance Policy is unconstitutional. Those claims will draw on evidence beyond the AR and likely require discovery. Depending on how the Court resolves this Motion, Plaintiffs expect to meet and confer with Defendants to propose a schedule and case management plan for resolving the remaining claims.

rationalizations, DOJ cannot demonstrate any “reasoned decisionmaking” to support its Policy; it is therefore arbitrary and capricious.

DOJ’s Policy—and the sprawling voter surveillance and purging regime it creates—is as dangerous as it is illegal. Underlying the Policy is DOJ’s alarming position that *every registered voter in the United States* is a “subject[.]” of DOJ’s nationwide dragnet “investigation into voter fraud,” even absent particularized suspicion. CRT-3356. Recognizing these dangers and the clear illegality of DOJ’s actions, most states and the District of Columbia have refused DOJ’s voter data demands. DOJ has sued those states to compel compliance, and every court so far to reach a motion to dismiss in those cases has ruled against DOJ.³ But some states have capitulated to DOJ’s demands, turning over their voters’ unredacted personal information without those voters’ prior knowledge or consent—including the Voter Plaintiffs and other Common Cause members. To protect these individuals and to prevent erroneous voter purges ahead of approaching midterm elections, Plaintiffs ask this Court to hold unlawful, vacate, and set aside DOJ’s Policy.

BACKGROUND

I. DOJ’s Voter List Maintenance Policy

A. President Trump’s efforts to “nationalize” elections and DOJ’s Voter List Maintenance Policy

DOJ’s Voter List Maintenance Policy flows directly from President Trump’s efforts to assert unprecedented—and unconstitutional—control over states’ maintenance of their voter rolls. President Trump repeatedly has declared his desire to “nationalize” or “take over” election

³ See *United States v. Weber*, 816 F. Supp. 3d 1168, 1182-95 (C.D. Cal. Jan. 15, 2026); *United States v. Oregon*, 2026 WL 318402, at *5-12 (D. Or. Feb. 5, 2026); *United States v. Benson*, 2026 WL 362789, at *2-10 (W.D. Mich. Feb. 10, 2026); *United States v. Galvin*, 2026 WL 972129, at *3-6 (D. Mass. Apr. 9, 2026); *United States v. Amore*, 2026 WL 1040637, at *4-6 (D.R.I. Apr. 17, 2026); *United States v. Fontes*, 2026 WL 1177244, at *2-7 (D. Ariz. Apr. 28, 2026).

administration from the states. *See* Hill Decl. ¶¶ 2-3 & Ex. 1. He has wrongly claimed that “the States are merely an ‘agent’ for the Federal Government in counting and tabulating ballots,” and that states “must do what the Federal Government, as represented by the President of the United States, tells them.” Hill Decl. Ex. 2. And President Trump has directed the Executive Branch to carry out this effort to nationalize election administration through two executive orders. *See* Hill Decl. Ex. 4, Exec. Order No. 14248, *Preserving and Protecting the Integrity of American Elections*, 90 Fed. Reg. 14005 (Mar. 25, 2025) (the “2025 Elections EO”); Hill Decl. Ex. 3, Exec. Order No. 14399, *Ensuring Citizenship Verification and Integrity in Federal Elections*, 91 Fed. Reg. 17125 (Mar. 31, 2026) (the “2026 Elections EO”).⁴ Among other things, the Executive Orders direct DOJ, DHS, and the Social Security Administration (“SSA”) to take various actions to “identify unqualified voters registered in the States,” including through expansive information sharing across agencies. Hill Decl. Ex. 4, 2025 Elections EO, §§ 2(b)-(c), 3(a); *see* Hill Decl. Ex. 3, 2026 Elections EO, § 2.

It is in this context that DOJ crafted and implemented its Voter List Maintenance Policy,⁵ which entails DOJ executing the following unauthorized, constituent actions:

- compiling all states’ Statewide Voter Registration Lists (“SVRLs”) on a generalized and categorical basis, rather than seeking certain states’ data based on specific allegations of list maintenance issues or to investigate specific alleged violations of federal law, *see, e.g., infra* note 7;

⁴ Courts nationwide, including in this District, have enjoined federal agencies from implementing key provisions of the 2025 Executive Order on the ground that they violate “the constitutional separation of powers.” *League of United Latin Am. Citizens (“LULAC II”) v. EOP*, 818 F. Supp. 3d 34, 57-58 (D.D.C. Jan. 30, 2026); *see also League of United Latin Am. Citizens (“LULAC I”) v. EOP*, 808 F. Supp. 3d 29, 79-80 (D.D.C. Oct. 31, 2025); *Washington v. Trump*, 2026 WL 73866, at *1 (W.D. Wash. Jan. 9, 2026); *California v. Trump*, 786 F. Supp. 3d 359, 371-72 (D. Mass. 2025).

⁵ CRT-3330 (“In response to the President’s [2025 Elections EO], . . . the Civil Rights Division . . . proposed to seek statewide voter lists and then to share the lists with Homeland Security Investigations or another unit within DOJ.”).

- consolidating all states' SVRLs in a centralized system of records at the Civil Rights Division ("CRT") titled "JUSTICE/CRT – 001, Central Civil Rights Division Index File and Associated Records," *see, e.g.*, CRT-0004, CRT-0024, CRT-2057, CRT-3387, to build a national record system with every state's SVRL;
- disclosing the voter data from the compiled SVRLs within and outside of DOJ, including to DHS, *see* CRT-0030; CRT-3399-3400; and private contractors, *see, e.g.*, CRT-0007, CRT-0027, CRT-2060, CRT-3396;
- comparing the voter data from the SVRLs against other federal datasets, such as DHS's SAVE system, *see, e.g.*, CRT-0030;
- testing, assessing, or analyzing the voter data in the SVRLs for "insufficiencies, inadequacies, deficiencies, anomalies, or concerns," *see, e.g.*, CRT-0005, CRT-0025, CRT-2058; and
- disclosing to the states the results of DOJ's testing, assessment, or analysis, with instructions that the states "clean" their SVRLs by "removing ineligible voters" identified by DOJ and then "resubmitting" the cleaned SVRLs to DOJ "to verify proper list maintenance has occurred," *see, e.g.*, CRT-0005, CRT-2058; *see also* Hill Decl. Ex. 5, p. 70 (*Amore* Hr'g Tr. at 70:12-25).

The AR reveals that DOJ has taken steps to implement each element of this Policy.

B. Compiling state voter registration lists

DOJ began implementing this Policy no later than May 2025, when it commenced its campaign to amass complete voter rolls from around the country. CRT-2432-2442. Assistant Attorney General for Civil Rights Harmeet Dhillon described this as a "comprehensive effort" to compile "the voter rolls from all states and the District of Columbia" so that CRT can conduct "voter hygiene" by "running" the states' voter rolls to identify purported deceased or non-citizen voters. *See* Hill Decl. ¶ 8. To execute this "comprehensive effort," DOJ sent near-identical demand letters to 49 states⁶ and the District of Columbia, seeking "all fields" contained in their full SVRLs,

⁶ North Dakota did not receive a demand letter as it is the only state that does not maintain a voter registration database. *See Brakebill v. Jaeger*, 905 F.3d 553, 556 (8th Cir. 2018) ("North Dakota has no voter registration requirement, so a resident may appear at the polls on election day and cast a ballot without any previous expression of desire to vote."). References in this brief to the SVRLs of "every" or "all" states thus do not include North Dakota.

including confidential data.⁷ SVRLs often contain sensitive Personal Identifying Information (“PII”), and indeed, DOJ’s letters demanded (among other things) “the last four digits of [each voter’s] social security number.” *Supra* note 7; *see also, e.g.*, CRT-2346; CRT-2401.

DOJ’s demand letters do not disclose what it is doing with the SVRL data. Although DOJ’s letters asserted that the “purpose” of its demands is to “ascertain [the states’] compliance with the list maintenance requirements of the NVRA and HAVA,” the letters contained no information about how DOJ is analyzing, protecting, or disclosing this information. *Supra* note 7. The letters did not contain OMB-issued control numbers required under the Paperwork Reduction Act for collections of information, nor did they disclose whether DOJ intended to create a new system of records or make use of an existing one to comply with the Privacy Act. *See id.* DOJ officials apparently believed that they had unfettered power to determine how to use the voter data. In internal communications, one official responsible for implementing the Policy asserted: “HAVA, NVRA, CRA - none of them require to give [sic] the states information about what we are going to do with the data. No judge will have authority to limit us beyond a promise of Federal law compliance.” CRT-3392.

⁷ *See* CRT-2346 (DOJ letter to Alaska); CRT-2400 (Arizona); CRT-2411 (Arkansas); CRT-2428 (California); CRT-2496 (Connecticut); CRT-2537 (Delaware); CRT-2558 (Florida); CRT-2572 (Georgia); CRT-2593 (Hawaii); CRT-2647 (Idaho); CRT-2684 (Illinois); CRT-2691 (Indiana); CRT-2702 (Iowa); CRT-2710 (Kansas); CRT-2714 (Kentucky); CRT-2744 (Louisiana); CRT-2759 (Maine); CRT-2770 (Maryland); CRT-2778 (Massachusetts); CRT-2790 (Michigan); CRT-2815 (Minnesota); CRT-2843 (Mississippi); CRT-2858 (Missouri); CRT-2872 (Montana); CRT-2891 (Nebraska); CRT-2905 (Nevada); CRT-2911 (New Hampshire); CRT-2927 (New Jersey); CRT-2945 (New Mexico); CRT-2955 (New York); CRT-2959 (North Carolina); CRT-2986 (Ohio); CRT-2989 (Oklahoma); CRT-3054 (Oregon); CRT-3064 (Pennsylvania); CRT-3071 (Rhode Island); CRT-3076 (South Carolina); CRT-3130 (South Dakota); CRT-3137 (Tennessee); CRT-3144 (Texas); CRT-3184 (Utah); CRT-3187 (Vermont); CRT-3193 (Virginia); CRT-3196 (Washington); CRT-2544 (Washington D.C.); CRT-3200 (West Virginia); CRT-3401 (Wyoming). Three States received communications that did not contain identical language but nonetheless requested the States’ full unredacted SVRLs. *See* CRT-2107 (Alabama); CRT-2431, CRT-2432 (Colorado); CRT-3229, CRT-3231 (Wisconsin).

Faced with DOJ’s sweeping demands, most states—at least 30 plus the District of Columbia (the “Non-Complying States”)—have refused to provide DOJ with voter files containing personal information that is not generally publicly available, and DOJ has sued them to force compliance. All six courts to rule on motions to dismiss have ruled against DOJ. *See supra* note 3. As one of those courts observed, “[t]he government’s request is unprecedented and illegal.” *Weber*, 816 F. Supp. 3d at 1174. But that has not stopped at least 18 states from acquiescing to DOJ’s data demands, including Alabama, Alaska, Arkansas, Florida, Indiana, Iowa, Kansas, Louisiana, Mississippi, Montana, Nebraska, Ohio, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, and Wyoming (the “Complying States”).⁸

C. Disclosing SVRLs to DHS and external third parties

Pursuant to DOJ’s Policy, after collecting SVRL data, DOJ will disclose personal voter registration information to DHS by bulk uploading the data to U.S. Citizenship and Immigration Service’s (“USCIS’s”) SAVE system, *see* CRT-0030-0040 (SAVE MOA between USCIS and DOJ), a system DHS itself admits cannot accurately verify the citizenship status of certain categories of U.S. citizens, *see infra* Background § I.D.⁹ And DOJ has executed a separate agreement with DHS’s Homeland Security Investigations (“HSI”) under which HSI will “enrich .

⁸ CRT-0458 (Alabama compliance letter); CRT-0001 (Alaska MOU); CRT-0946 (Arkansas compliance letter); CRT-1437 (Florida compliance letter); CRT-1511 (Indiana compliance letter); CRT-3259 (Iowa compliance letter); CRT-1533 (Kansas compliance letter); CRT-1622 (Louisiana compliance letter); CRT-3261 (Mississippi compliance letter); CRT-3263 (Montana data transfer email); CRT-3265 (Nebraska compliance letter); CRT-3126 (Ohio compliance letter); CRT-0011 (Oklahoma compliance settlement); CRT-0021 (South Carolina MOU); CRT-1994 (South Dakota compliance letter); CRT-1996, CRT-2002 (Tennessee compliance letters); CRT-2036 (Texas MOU); CRT-3404 (Wyoming compliance letter).

⁹ DHS stores and retains records uploaded into SAVE for a minimum of ten years. *See* DHS, System of Records Notice, 90 Fed. Reg. 48948, 48954-55 (Oct. 31, 2025).

. . SVRL datasets” provided by DOJ “with DHS records to allow for vetting via the SAVE system” and then “return” them for DOJ to “query the SAVE system.” CRT-3399-3400.

DOJ’s Memoranda of Understanding with Alaska, South Carolina, and Texas also reveal that DOJ may disclose voter data *outside* the government to “a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department’s list maintenance verification procedures.” CRT-0007 (Alaska MOU); CRT-0027 (South Carolina MOU); CRT-2060 (Texas MOU); *see also* CRT-3396 (internal DOJ email stating that when DOJ receives voter data it may “require processing information in new ways,” including “[p]otential analysis of ingested data by [a] litigative consultant”). DOJ has not identified how those contractors will use the highly sensitive data or if any special safeguards are in place.

D. Using DHS’s error-riddled SAVE system to check voter eligibility

Under its Voter List Maintenance Policy, DOJ will run states’ entire SVRLs through SAVE to conduct citizenship checks with the explicit aim of identifying individuals whom DOJ will demand that states remove from their voter rolls. *See* CRT-0030-0040; Hill Decl. Ex. 5 (*Amore* Hr’g Tr. at 50:22-23). But SAVE was not designed to check voter eligibility,¹⁰ and is unreliable. As DHS has acknowledged, relying on SAVE poses serious risks of falsely flagging U.S. citizens as non-citizens, many of which DHS has not been able to mitigate. *See* Hill Decl. Exs. 13-16 (DHS-AR-240-243; DHS-AR-260; DHS-AR-302; DHS-AR-484-85).

As the AR here confirms, SAVE cannot reliably confirm citizenship and is especially unreliable for citizens born outside of the United States (e.g., naturalized, derived, and acquired

¹⁰ Congress established the system to verify whether non-citizens are entitled to certain government benefits. *See* Immigration Reform Control Act of 1986, Pub. L. No. 99-603, title I, §121(c)(1), 100 Stat. 3359, 3391 (1986), *codified at* 42 U.S.C. § 1320b-7 note; *id.* § 121(a)(1)(C), 100 Stat. at 3384-86 (1986), *codified at* 42 U.S.C. § 1320b-7(d) (§ 121 titled “Verification of Immigration Status of Aliens Applying for Benefits under Certain Programs”).

citizens).¹¹ For instance, DHS admits that “SAVE may only be able to verify acquired U.S. citizenship in certain situations,” and if DOJ queries “an individual with acquired citizenship who has not applied for a Certificate of Citizenship with [DHS], . . . SAVE may not be able to confirm that individual’s acquired citizenship.” CRT-0032 (SAVE MOA between USCIS and DOJ). Similarly, SAVE incorporates data collected by the Social Security Administration (“SSA”) that SSA has long recognized is incomplete and unreliable for verifying citizenship status of citizens born outside the U.S., because the data only reflects the person’s citizenship status when they applied for an SSN, and does not automatically update if the person later becomes a citizen. *See* Hill Decl. Exs. 17-19 (SSA-AR-44; SSA-AR-103; July 13, 2023, Letter from SSA Office of Gen. Counsel to Fair Elections Ctr. 2). A 2006 internal audit estimated that SSA’s citizenship data inaccurately identified about 3.3 million citizens as non-citizens “because they had become U.S. citizens after obtaining their SSN.” Hill Decl. Ex. 20 (SSA IG Report iii).

In its most recent Privacy Impact Assessment for SAVE, DHS noted that the system “may share inaccurate information with registered agencies, which could in turn impact a registered user agency’s eligibility determination for an individual,” and that “due to misspelling of names, transposed numbers, or incomplete information, the SAVE Program may produce inaccurate results.” *See* Hill Decl. Ex. 13 (DHS-AR-000240-41); *accord* CRT-0032; Hill Decl. Exs. 14-15, 17-18 (DHS-AR-260, recognizing SAVE’s “[s]hortfalls in data accuracy”; DHS-AR-302, stating same; SSA-AR-44, stating “citizenship information in SSA’s records might not be current”; SSA-AR-103, stating same). These concerns are not hypothetical: Plaintiff Anthony Nel and another

¹¹ Acquired citizenship is “[c]itizenship conferred at birth on children born abroad to a U.S. citizen parent(s).” *Acquired citizenship*, USCIS Glossary of Terms, <https://perma.cc/8AB4-9LAX>. Derived citizenship is “[c]itizenship conveyed to children through the naturalization of their parents or, under certain circumstances, to foreign-born children adopted by U.S. citizen parents.” *Derivative citizenship*, USCIS Glossary of Terms, <https://perma.cc/7SXE-ZTYT>.

Common Cause member declarant suffered wrongful removal from the voter rolls after their state relied on SAVE for voter list maintenance, and another Common Cause member declarant was forced to provide documentary proof of citizenship (“DPOC”) to retain their voter registration. *See infra* Argument § I.¹²

E. Directing states to remove voters

The AR shows that if DOJ’s Voter List Maintenance Policy “reveals that an alien unlawfully has registered to vote or voted in an election, the [Civil Rights] Division may seek to strike the alien’s name from the voter registration list for future elections, refer the alien for prosecution, or both.” CRT-3334. Indeed, DOJ has executed Memoranda of Understanding with at least three of the eighteen Complying States providing that DOJ will notify the state of “any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns [] the Justice Department found when testing, assessing, and analyzing your state’s VRL [voter registration list] for NVRA and HAVA compliance, i.e., that [the] state’s VRL only includes eligible voters,” and purporting to commit the states, “within forty-five (45) days of receiving the notice from the Justice Department” to “remov[e]” putatively ineligible voters. *See* CRT-0005 (Alaska); CRT-2058 (Texas); CRT-0025 (South Carolina).¹³ DOJ’s representations to courts in

¹² The public record reveals that improper removals based on SAVE use are widespread. *See* Jen Fifield & Zach Despart, “*Not Ready for Prime Time.*” *A Federal Tool to Check Voter Citizenship Keeps Making Mistakes*, ProPublica & Texas Tribune (Feb. 13, 2026), <https://perma.cc/PR4Q-67NR>.

¹³ The MOUs with Alaska and Texas state that commitment slightly differently than the MOU with South Carolina. Alaska and Texas each commit to “clean [their] VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance.” CRT-0005; CRT-2058. The South Carolina MOU commits the state to “remove any ineligible voters as identified by the Justice Department and confirmed by the [State Election Commission].” CRT-0025. But all MOUs in the AR reveal the crux of the Voter List Maintenance Policy: DOJ’s expectation that it will analyze a state’s voter roll and dictate the voters that the states will then remove from the SVRLs.

litigation with Non-Complying States likewise confirm that DOJ intends to “run these lists against other databases to be able to tell if there are bad registrations on their rolls” and if DOJ identifies a voter with a purportedly “bad registration,” DOJ will contact the states to “verify . . . they have removed [that voter] from the rolls.” Hill Decl. Ex. 5 (*Amore* Hr’g Tr. at 70:12-25).

F. The Administrative Record

On May 7, 2026, Defendants produced a certified administrative record totaling 522 documents, and on May 18, they supplemented the AR with an additional 34 documents. However, none of those documents pre-dates DOJ’s implementation of the Policy in May 2025, when Defendants began demanding states’ SVRLs. As the AR consists exclusively of documents post-dating the Policy’s roll-out, no concrete reasoning, studies, or public engagement plausibly influenced the agency’s decision-making before the Policy’s implementation.

II. Impact of DOJ’s Voter List Maintenance Policy on the Plaintiffs

DOJ’s Voter List Maintenance Policy has inflicted and will continue to inflict serious harms on Plaintiffs. *See infra* Argument § I. For the Voter Plaintiffs and other Common Cause members registered to vote in states that have supplied their SVRLs to DOJ, the Voter List Maintenance Policy has caused pervasive unauthorized uses and disclosures of their sensitive personal data across various federal agencies without their consent. *See id.* And DOJ’s unprecedented centralization of their personal information in a single federal system of records exposes the voters to profound data-security risks, including data theft or doxxing. *See id.* For Common Cause, DOJ’s Policy has directly impaired its mission-critical voter protection services and educational programs and forced it to expend its scarce resources to counteract that harm. *See id.* And all Plaintiffs have been deprived of statutorily guaranteed information and opportunities to comment on the Policy *before* it went into effect. *See id.*

LEGAL STANDARD

When reviewing agency action under the APA, “[s]ummary judgment . . . serves as the mechanism for deciding, as a matter of law, whether the agency action is supported by the administrative record and otherwise consistent with the APA standard of review.” *Stuttering Found. of Am. v. Springer*, 498 F. Supp. 2d 203, 207 (D.D.C. 2007). “[T]he district judge sits as an appellate tribunal[] [and] [t]he ‘entire case’ on review is a question of law.” *Am. Bioscience, Inc. v. Thompson*, 269 F.3d 1077, 1083 (D.C. Cir. 2001).

ARGUMENT

DOJ’s Voter List Maintenance Policy far exceeds the agency’s statutory authority and violates multiple laws designed to protect Americans’ privacy and data security. Plaintiffs, who are directly harmed by DOJ’s unlawful actions in many ways, are entitled to summary judgment on Counts I, VI, VII, and VIII of their Complaint.

I. Plaintiffs have standing

To establish Article III standing, a plaintiff must show that (1) “it has suffered an injury in fact” that is “concrete and particularized” and “actual or imminent,” (2) “the injury is fairly traceable to the challenged action of the defendant,” and (3) “it is likely . . . that the injury will be redressed by a favorable decision.” *Friends of the Earth, Inc. v. Laidlaw Env’t Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000) (internal citation omitted). Here, Plaintiffs have demonstrated multiple grounds for standing to challenge DOJ’s unlawful Voter List Maintenance Policy.

Organizational standing. Common Cause has organizational standing on its own behalf, because DOJ’s Voter List Maintenance Policy “‘directly affect[s] and interfere[s] with [its] core business activities’” of providing services and educational resources to voters and its mission of promoting political participation. *See Ctr. for Biological Diversity v. Dep’t of Interior*, 144 F.4th

296, 315 (D.C. Cir. 2025) (quoting *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 395 (2024)); see also *League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 9 (D.C. Cir. 2016).

Common Cause is a national, nonpartisan organization with nearly one million members across all 50 states. Nunez Decl. ¶ 5, 7. Its mission is to create open, honest, and accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all people to make their voices heard in the political process. Nunez Decl. ¶ 8. As part of its mission, Common Cause devotes significant resources to promoting voter participation and expends resources deploying and supporting on-the-ground staff, including in Complying States such as Texas, Ohio, Nebraska, and Indiana, to carry out its mission. Nunez Decl. ¶¶ 7-12; Geis Decl. ¶¶ 5-7; Vaughn Decl. ¶¶ 5-7; Turcer Decl. ¶¶ 5-7. Common Cause's efforts in those states include monitoring changes in voter registration and election procedures and administration at the state and local level; educating the public about changes in voting and election procedures; direct outreach to encourage people to register and vote; assisting, training and supporting partner organizations that conduct voter registration; and conducting or facilitating poll observation and other election protection programs to ensure that election procedures are followed, that eligible voters are able to vote, and that voters who encounter trouble at the polls have access to assistance. Nunez Decl. ¶¶ 10-13; Vaughn Decl. ¶¶ 7, 10-11, 17; Gutierrez Decl. ¶¶ 10-13; Geis Decl. ¶¶ 7-9; Turcer Decl. ¶¶ 7, 10-15. Common Cause devotes resources, including money, staff and volunteer time, and strategic bandwidth to plan and execute these programs. *Id.*

Among other impacts, DOJ's Voter List Maintenance Policy will disrupt Common Cause's existing voter education and protection efforts in three critical ways, hampering its ability to provide those core services and causing it to expend additional resources to accomplish its goal of

increasing political engagement and participation. Nunez Decl. ¶¶ 15-16; Vaughn Decl. ¶¶ 9-22; Geis Decl. ¶¶ 8-16; Turcer Decl. ¶¶ 9-16; Gutierrez Decl. ¶¶ 9-11, 15-20.

First, DOJ's actions have increased public concern, requiring Common Cause to divert resources that it would otherwise spend on existing programming—including to register and engage more voters—to instead investigate the scope of DOJ's new Policy and to educate registered and potential voters about the risks and benefits of voting in the face of DOJ's actions. For example, because DOJ is collecting voter data and sharing it with DHS, many more members of the public have expressed concern about how the federal government will use their personal data, including for purposes of retaliation. Geis Decl. ¶ 10; Gutierrez ¶ 15; Vaughn ¶¶ 12-13. In Common Cause's experience, naturalized and derived citizens are more likely to have those concerns. Nunez Decl. ¶ 16; Geis Decl. ¶ 10; Vaughn Decl. ¶¶ 11-12. Common Cause therefore has expended (and will be forced to expend more of) its limited resources (i) to gather necessary information on DOJ's secretive process, (ii) to educate potential registrants, voters, volunteers, and civil society partners about the uses and misuses of voters' private data, and (iii) to address voters' legitimate fears about whether their personal data is secure and whether their political participation will come at a price. Nunez Decl. ¶¶ 16, 20-21; Vaughn Decl. ¶¶ 15, 21-22; Gutierrez Decl. ¶¶ 9-11, 15-18; Geis Decl. ¶¶ 10-12, 16; Turcer Decl. ¶¶ 13-16.

Second, DOJ's actions have undermined the effectiveness of Common Cause's core activities promoting political participation. In addition to chilling eligible or registered voters, such as naturalized citizens, from participating in the political process, DOJ's Voter List Maintenance Policy contemplates removing registered voters—people that the states have determined to be qualified—based on data acknowledged to be unreliable. *See supra* Background §§ I.D-E. That

directly undermines Common Cause’s work “to ensure that once registered, all voters can cast a ballot.” Nunez Decl. ¶¶ 8, 12.

Third, Common Cause, as it has done in response to past efforts to purge voters using unreliable data, must divert resources to counteract the direct impact of the Policy itself to ensure that voters are not wrongly disenfranchised. In the Complying States, Common Cause will have to divert resources to educate the public about checking their voter registrations and train volunteers to identify voters whose registrations have been improperly purged due to the Voter List Maintenance Policy and assist those voters in restoring their registration. Nunez Decl. ¶ 21; Vaughn Decl. ¶¶ 20-22; Gutierrez Decl. ¶¶ 17-20; Geis Decl. ¶¶ 12, 16. All of this will leave Common Cause with fewer resources to devote to its existing core organizational activities. *Id.*

Common Cause has therefore demonstrated both “injury to its organizational interests” and that it has “used its resources to counteract that harm.” *Indep. Mkt. Monitor for PJM v. FERC*, 162 F.4th 1167, 1172 (D.C. Cir. 2025). And these injuries are heightened by the ongoing election cycle, for once an election passes, “there can be no do over and no redress.” *Newby*, 838 F.3d at 9 (quoting *League of Women Voters of N.C. v. North Carolina*, 769 F.3d 224, 247 (4th Cir. 2014)).

Informational standing. Common Cause also has informational standing on its own behalf. “To prove an informational injury, a plaintiff must show that (1) it has been deprived of information that, on its interpretation, a statute requires the government or a third party to disclose to it, and (2) it suffers, by being denied access to that information, the type of harm Congress sought to prevent by requiring disclosure.” *Ctr. for Biological Diversity v. U.S. Int’l Dev. Fin. Corp.*, 77 F.4th 679, 685 (D.C. Cir. 2023) (citation modified). Here, DOJ has deprived Common Cause of critical information required by the public notice provisions of the Privacy Act and PRA. *See infra* Argument §§ III.B-C. Without these statutorily mandated disclosures, Common Cause

must undertake costly and time-intensive efforts to obtain information about DOJ's use of voter data so that it may be properly informed when engaging in voter education and other advocacy efforts. *See* Vaughn Decl. ¶¶ 15-19; Turcer Decl. ¶¶ 11, 13-14, 16; Gutierrez Decl. ¶¶ 15-16; Geis Decl. ¶¶ 9, 14; Nunez Decl. ¶¶ 18-19, 22; *see also United to Protect Democracy v. Presidential Advisory Comm'n on Election Integrity*, 288 F. Supp. 3d 99, 106-10 (D.D.C. 2017) (voting rights groups were injured by deprivation of information mandated by PRA regarding federal collection of voter data from states). And this injury is heightened by the "critical public need for timely access to . . . information" about DOJ's "widespread effort to gather sensitive information about vast numbers of registered voters," which will "shed light on important matters concerning voter privacy and the separation of powers in the inherently time-limited context of an active election cycle." *CREW v. DOJ*, --- F. Supp. 3d ---, No. 25-cv-4426, 2026 WL 472589, at *1, *12-13 (D.D.C. Feb. 19, 2026).

Associational and Voter Plaintiff standing. Common Cause has associational standing on behalf of its members, based on DOJ Policy's harms to its members' privacy, voting, informational, and procedural rights. *See Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 600 U.S. 181, 199 (2023). And the Voter Plaintiffs have standing in their own right based on the same injuries.

As to **privacy injuries**, DOJ's wrongful use and disclosure of the Voter Plaintiffs' and other Common Cause members' protected voter registration data inflicts harms that are sufficiently "concrete" because they are a "close . . . analogue" to the harms vindicated by the "common law tort of intrusion upon seclusion." *AFSCME v. SSA*, 172 F.4th 361, 368 (4th Cir. 2026) (en banc) (quoting *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424-25 (2021)); *see also LULAC II*, 818 F. Supp. 3d at 110 (unauthorized inter-governmental "sharing of sensitive [voter registration]

information” through SAVE system bore a sufficiently “close relationship” to “intrusion upon seclusion”); *accord AFL-CIO v. Dep’t of Lab.*, 778 F. Supp. 3d 56, 73 (D.D.C. 2025). When each of the Voter Plaintiffs and other Common Cause members registered to vote, they provided sensitive personal information with the expectation that it would be used only for the purpose of registering to vote. Each expected this information to be kept private when they supplied it to state election officials, with assurances in state privacy laws and the typical redactions in public versions of the voter file. *See, e.g.*, Nel Decl. ¶¶ 35-38, 47, 51; Duckworth Decl. ¶¶ 8-10; R. Nasrullah Decl. ¶¶ 8-10; Smith Decl. ¶¶ 10-13; A. Doe Decl. ¶ 20; B. Doe Decl. ¶ 39; Mosse Decl. ¶¶ 11-14; M. Nasrullah Decl. ¶¶ 11-14. They did not consent to it to being obtained, stored, and used by DOJ. *Id.* Nor did they consent to it being shared with, stored, and used by other federal agencies, such as DHS, private contractors and third parties. *Id.* DOJ’s Voter List Maintenance Policy also exposes the Voter Plaintiffs and other Common Cause members to the risk that their sensitive data will be misused or stolen. Nel Decl. ¶¶ 39-41, 51-53; Duckworth Decl. ¶¶ 20-24, 29-30; R. Nasrullah Decl. ¶¶ 19-28, 32-33; Smith Decl. ¶¶ 23-27, 30-31; A. Doe Decl. ¶¶ 23-25, 37-39; B. Doe Decl. ¶¶ 41-43, 53-55; Mosse Decl. ¶¶ 29-34, 40-41; M. Nasrullah Decl. ¶¶ 29-35, 39-41. They reasonably fear that DOJ’s improper centralization and misuse of their sensitive SVRL data exposes them to risks of identity theft, doxxing, and fraud. Nel Decl. ¶¶ 40-41; Duckworth Decl. ¶¶ 20, 24; R. Nasrullah Decl. ¶¶ 19-20. Smith Decl. ¶¶ 23-25; A. Doe Decl. ¶¶ 24-25; B. Doe Decl. ¶¶ 42-43; Mosse Decl. ¶¶ 29-32; M. Nasrullah Decl. ¶ 39.

Common Cause’s members and the Voter Plaintiffs are also suffering cognizable **voting-related injuries** due to Voter List Maintenance Policy’s harms to and burdens on their “fundamental right to vote,” which is a “cornerstone premise of democracy.” *Mi Familia Vota v. Fontes*, 129 F.4th 691, 708 n.3 (9th Cir. 2025) (citing cases). Courts zealously “guard” and “firmly

and unequivocally reject[]” burdens on the right to vote. *Id.* Even an “increased risk” of disenfranchisement can make an injury “sufficiently ‘imminent’ for standing purposes.” *Richardson v. Trump*, 496 F. Supp. 3d 165, 179 (D.D.C. 2020) (quoting *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017)) (internal citation omitted).

Certain Voter Plaintiffs and other Common Cause members face an elevated risk of being erroneously removed from the voter rolls due to DOJ’s Voter List Maintenance Policy. *See* Nunez Decl. ¶ 14. For example, Plaintiff Nel is a derived U.S. citizen and one of many Texas voters whose voter registration has already been wrongly cancelled by local election officials in Texas due to their use of the flawed SAVE system for statewide voter list maintenance. Nel Decl. ¶¶ 3-6, 13-22, 25-26. Common Cause member Bailey Doe is a naturalized citizen whose voter registration was wrongly canceled due to Texas’s use of SAVE and who was prevented from voting, and thereby disenfranchised, in the March 2026 primary election. B. Doe Decl. ¶¶ 11-31. And Common Cause member Alex Doe is a derived citizen who was forced to provide documentary proof of citizenship to retain their voter registration due to Texas’s use of SAVE. A. Doe Decl. ¶¶ 11-14. Because the federal government has not updated these voters’ citizenship data in SAVE, *see* Nel Decl. ¶ 43; B. Doe Decl. ¶¶ 45, 47; A. Doe Decl. ¶¶ 27, 29, it is likely that DOJ’s usage of SAVE for its “list maintenance verification procedures” will cause these voters to again be misidentified as non-citizens and again have their right to vote burdened. CRT-2060. Indeed, DOJ’s MOA with DHS to use SAVE for voter verification explicitly contemplates that voters will be forced to provide “proof of U.S. citizenship” if SAVE’s unreliable data and methods fail to confirm their citizenship. CRT-0033-0034.

Procedural standing. All Plaintiffs have procedural standing due to DOJ violations of the Privacy Act’s and PRA’s notice-and-comment requirements in ways that impair their above-

described “concrete interests in a personal way.” *Mendoza v. Perez*, 754 F.3d 1002, 1010, 1013 (D.C. Cir. 2014).

Causation and redressability. But for DOJ’s unlawful efforts to stockpile and disclose millions of Americans’ sensitive voter registration data to create a sprawling new voter purge regime, none of Plaintiffs’ injuries would have occurred. “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). And as explained below, *see infra* Argument § IV, Plaintiffs’ requested relief is “likely” to redress their injuries. *Diamond Alt. Energy, LLC v. EPA*, 606 U.S. 100, 114 (2025); *see also Massachusetts v. EPA*, 549 U.S. 497, 526 (2007) (finding standing where the “risk [of harm] would be reduced to some extent if petitioners received the relief they seek”).

II. Plaintiffs challenge final agency action

DOJ’s Voter List Maintenance Policy, as well as the associated policies and agreements, constitutes “final agency action” subject to APA review, because the Policy “mark[s] the consummation of the agency’s decisionmaking process” and is an action by “which rights or obligations have been determined, or from which legal consequences will flow.” *Bennett v. Spear*, 520 U.S. 154, 178 (1997) (internal citations omitted). DOJ’s Policy entails demanding, compiling, and consolidating SVRL data from every state; disclosing and comparing voter data from the compiled SVRLs within and outside of DOJ; testing, assessing, or analyzing the data for “insufficiencies” and “inadequacies;” and purporting to require states to remove those ineligible voters identified by DOJ to “clean” their voter rolls. *See supra* Background §§ I.A, E. The AR makes clear that DOJ has definitively adopted the Policy in ways that have legal consequences, including binding MOUs and new data practices. *See, e.g., Venetian Casino Resort, LLC v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008) (agency’s decision “to adopt a policy of disclosing confidential

information without notice” is “surely a consummation of the agency’s decisionmaking process”) (internal citation omitted); *Nat’l Ass’n of Home Builders v. Norton*, 298 F. Supp. 2d 68, 76 (D.D.C. 2003) (agency “actively soliciting and reviewing input” and “data collected” is final agency action), *aff’d*, 415 F.3d 8 (D.C. Cir. 2005).

III. Plaintiffs are entitled to summary judgment on Counts I, VI, VII, and VIII of the Complaint

DOJ’s Voter List Maintenance Policy vastly exceeds the agency’s statutory authority, *see* Compl. ¶¶ 158-65 (Count I), violates the Privacy Act’s procedural and substantive safeguards, *see id.* ¶¶ 188-202 (Count VI), violates the PRA’s notice-and-comment procedures, *see id.* ¶¶ 203-17 (Count VII), and was arbitrary and capricious, *see id.* ¶¶ 218-20 (Count VIII). Each claim provides an independent basis to enter summary judgment for Plaintiffs and to hold unlawful, vacate, and set aside DOJ’s Policy under the APA.

A. DOJ’s Voter List Maintenance Policy lacks statutory authorization (Count I)

DOJ has asserted that NVRA and HAVA authorize the Voter List Maintenance Policy. *See supra* note 7. But DOJ is wrong: neither the NVRA, nor HAVA, nor any other law, authorizes its actions here. The NVRA and HAVA are part of a longstanding history of election administration (and in particular, voter list maintenance) being a responsibility of the states. To depart from that established practice—and authorize the momentous power of federalizing voter list maintenance—would require a clear statement from Congress. DOJ can point to no such statement in either the NVRA or HAVA. To the contrary, each law expressly limits DOJ’s role to bringing enforcement actions if states lack “reasonable” processes for removing ineligible voters. 52 U.S.C. § 20507(a)(4) (NVRA); § 21083(a)(4)(A) (HAVA). Neither law permits DOJ to cast a dragnet over virtually every jurisdiction’s voter list or to dictate the eligibility of every voter down to the individual person.

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) (citation modified); accord *Marin Audubon Soc’y v. FAA*, 121 F.4th 902, 912 (D.C. Cir. 2024). “And if an agency acts without statutory authority, then a court must set that action aside” under the APA. *Drs. for Am. v. OPM*, 793 F. Supp. 3d 112, 143 (D.D.C. 2025). “To determine ‘whether an agency has acted within its statutory authority,’ [courts] use ‘the traditional tools of statutory construction.’” *U.S. Sugar Corp. v. EPA*, 113 F.4th 984, 997 (D.C. Cir. 2024) (quoting *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 403 (2024)). And the Court must “interpret the words of these statutes in light of the purposes Congress sought to serve.” *Chapman v. Hou. Welfare Rts. Org.*, 441 U.S. 600, 608 (1979).

In our constitutional order, the responsibility for voter registration has long resided with the states. See, e.g., *Roudebush v. Hartke*, 405 U.S. 15, 24 (1972); *LULAC I*, 808 F. Supp. 3d at 43 (“By default, States are tasked with regulating, among other things, voter registration.”). The Elections Clause vests power in *Congress* to override that default setting, and “Congress must speak clearly if it intends to delegate any part of that power to the Executive Branch.” *LULAC II*, 818 F. Supp. 3d at 100 (citing *West Virginia v. EPA*, 597 U.S. 697, 723 (2022)). A clear expression from Congress is especially important here, because the administration of this nation’s elections is undoubtedly a question of “vast economic and political significance.” See *Ala. Ass’n of Realtors v. HHS*, 594 U.S. 758, 764 (2021) (citation modified). Defendants, however, can point to no statement from Congress, clear or otherwise, that authorizes their sprawling takeover of voter list maintenance.

The plain text of both the NVRA and HAVA makes clear that the states—not federal agencies—are responsible for voter list maintenance. Under the NVRA, “each *State* shall . . . conduct a general program that makes a reasonable effort to remove the names of ineligible voters

from the official lists of eligible voters[.]” 52 U.S.C. § 20507(a)(4) (emphasis added); *Bellitto v. Snipes*, 935 F.3d 1192, 1195 (11th Cir. 2019) (explaining that NVRA “centralizes” voter rolls list maintenance “responsibility in the state”); *accord Pub. Int. Legal Found., Inc. v. Nago*, --- F.4th ---, 2026 WL 1144703, at *2 (9th Cir. Apr. 28, 2026).

Likewise, under HAVA, “each *State* . . . shall implement . . . a *single, uniform, official, centralized*, interactive computerized statewide voter registration list defined, maintained, and administered *at the State level*.” 52 U.S.C. § 21083(a)(1)(A) (emphasis added); *Am. Civ. Rts. Union v. Phila. City Comm’rs*, 872 F.3d 175, 180-81 (3d Cir. 2017). Specific to list maintenance, each state is required to have a “system . . . that makes a reasonable effort to remove registrants who are ineligible to vote from the official list of eligible voters[.]” 52 U.S.C.A. § 21083(a)(4)(A). “Nowhere in the language or structure of HAVA as a whole is there any indication that the Congress intended to strip from the States their traditional responsibility to administer elections[.]” *Sandusky Cnty. Democratic Party v. Blackwell*, 387 F.3d 565, 576 (6th Cir. 2004).

DOJ has a defined, secondary role under the NVRA and HAVA: to bring enforcement actions to ensure that the statutes’ requirements are followed. 52 U.S.C. §§ 20510(a), 20511 (NVRA); §§ 21111, 21144 (HAVA). Specific to list maintenance obligations under these laws, states must have a “program” or “system” that “makes a reasonable effort” to remove ineligible voters. 52 U.S.C. § 20507(a)(4) (NVRA); § 21083(a)(4)(A) (HAVA). DOJ’s enforcement authority in this context is therefore limited to circumstances when a state’s list maintenance *processes* are not “reasonable.” *Id.* Nowhere does the NVRA or HAVA permit DOJ to create a parallel system of voter registration databases and supervise the qualification of voters down to the person, as described in the already executed MOUs and by DOJ elsewhere. *See supra* Background §§ 1.A, E. Indeed, HAVA contemplates a “single” voter list for each state,

“administered at the State level.” 52 U.S.C. § 21083(a)(1)(A). And more specifically, nothing in the NVRA or HAVA gives DOJ the authority, on a dragnet basis and without any particularized investigatory purpose, to:

- “conduct searches that assess the List Maintenance of voter registration lists,” CRT-3386;
- “test [states’] lists,” CRT-3384, and “identify . . . areas that may require maintenance,” *id.*;
- facilitate DOJ’s “analysis of ingested data by litigative consultant,” CRT-3396; *see also* CRT-0007; CRT-0027, CRT-2060;
- “seek to strike [an] alien’s name from the voter registration list for future elections,” CRT-3334, dictate how states “clean” their own voter rolls, CRT-0005; CRT-2058; Hill Decl. Ex. 5, p. 70 (*Amore* Hr’g Tr. at 70:12-25), or
- require that, after list maintenance, states “resubmit” their SVRLs to DOJ so DOJ can “verify proper list maintenance has occurred,” CRT-0005; CRT-2058.

Instead, “federal law largely leaves the finer details of list maintenance to the States’ discretion.”

Galvin, 2026 WL 972129, at *1.

Moreover, the undisputed facts show that DOJ’s sweeping operation under the Policy bears no resemblance to any reasonable definition of an individualized investigation. DOJ has launched an all-encompassing effort to capture voter data from everywhere it exists in the country, recycling virtually identical, cookie-cutter demands across each jurisdiction and without alleging any specific misconduct. *See supra* note 7. Indeed, DOJ’s Policy explicitly presumes that *every registered voter in the country* is a ““subject[]” of DOJ’s nationwide dragnet “investigation into voter fraud”—even absent particularized suspicion. CRT-3356 & n.27 (quoting Justice Manual § 9-11.151 (Jan. 2020), <https://perma.cc/9HVT-HLZC>). Such a Policy is antithetical to valid enforcement actions, which are predicated on individualized suspicions of specific violations of law. “Neither the NVRA nor HAVA authorize . . . the kind of fishing expedition [DOJ] seeks here.” *See United States v. Amore*, 2026 WL 1040637, at *6 (D.R.I. Apr. 17, 2026).

DOJ's actions also undermine the NVRA's purpose. *See* 52 U.S.C. § 20501(b) (stating that NVRA's goal is "to establish procedures that will increase the number of eligible citizens who register to vote" and "enhance[] the participation of eligible citizens as voters"). For instance, the NVRA builds in significant protections for voters, requiring that, once identified, certain potentially ineligible voters *must* stay on the rolls for two election cycles, to limit the likelihood of removing eligible voters by mistake. *Id.* § 20507(d)(1)(B). Under DOJ's MOUs' terms, however, once federal officials identify supposed "ineligible voters," states are required to "remov[e]" these voters "within forty-five (45) days." CRT-0005 (Alaska MOU); CRT-2058 (Texas MOU). Critically, these removals are required notwithstanding the NVRA's procedural protections for voters, including the statute's bar on systematic removals of voters within 90 days of an election, 52 U.S.C. § 20507. DOJ seeks to "use civil rights legislation which was enacted for an entirely different purpose to amass and retain an unprecedented amount of confidential voter data," going "far beyond what Congress intended when it passed the underlying legislation." *Weber*, 816 F. Supp. 3d at 1195.

Finally, DOJ's interpretation of the NVRA and HAVA has no historical basis, and courts should "hesitate" when an agency "'claim[s] to discover in . . . long-extant statute[s] 'an unheralded power' representing a 'transformative expansion [of its] . . . authority.'" *West Virginia*, 597 U.S. at 724 (citation omitted). Congress enacted the NVRA in 1993 and HAVA in 2002. Despite these laws being in place for decades, never before has DOJ asserted that they empower the agency to centralize hundreds of millions of Americans' sensitive voter registration data in a single system of records, disclose that data to third parties, compare it to other databases, analyze it, and then compel states to purge their voter rolls of purportedly "ineligible voters" identified by DOJ's undisclosed methodology. The indisputable "'lack of historical precedent'" for DOJ's

actions, “coupled with the breadth of authority that [DOJ] now claims, is a ‘telling indication’” that they “extend[] beyond the agency’s legitimate reach.” *Nat’l Fed’n of Indep. Bus. v. Dep’t of Lab.*, 595 U.S. 109, 119 (2022) (per curiam).

B. DOJ’s Voter List Maintenance Policy violates the Privacy Act (Count VI)

Under its Voter List Maintenance Policy, DOJ is centralizing vast volumes of sensitive individual voter registration data in a single federal system of records at CRT. DOJ is also disclosing tens of millions of individuals’ SVRL data across federal agencies and contractors, including to DHS to run mass citizenship checks through its flawed SAVE system, in substantially new and different ways without those individuals’ consent or statutory authorization. In doing so, DOJ has violated the Privacy Act’s core procedural and substantive protections. As one court recently found, DOJ’s creation of a “‘centralized Federal information system[]’” of Americans’ personal voting data endangers the “privacy” of millions of Americans and brings to life the very fears “that animated Congress to pass the Privacy Act—threats to American democracy amidst erosion of public trust regarding the Executive’s use of sensitive data.” *Weber*, 816 F. Supp. 3d at 1194 (quoting S. Comm. on Gov’t Operations and H.R. Comm. on Gov’t Operations, 94th Cong., 2d Sess., Source Book on Privacy at 168 (1976)).¹⁴

1. DOJ violated the Privacy Act’s notice-and-comment requirements for revising systems of records

In amassing for the first time millions of Americans’ voter registration data in one system *and* in using that system in substantially different ways than it had previously been used, DOJ flouted the Privacy Act’s notice-and-comment requirements and thus acted “without observance

¹⁴ The APA provides a remedy for DOJ’s violations of the Privacy Act. *See, e.g., LULAC II*, 818 F. Supp. 3d at 110-113 (APA remedy to challenge SAVE overhaul); *AFL-CIO*, 778 F. Supp. 3d at 81 (DOGE data access).

of procedure required by law.” 5 U.S.C. § 706(2)(D); *see* Compl. ¶¶ 190-95.

The Privacy Act requires agencies to publish a system of records notice (“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). “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, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 7 & 12 (2016), <https://perma.cc/N9QK-SDLE> (“OMB Circular No. A-108”). Agencies “shall” review and consider “public comments on a published SORN.” *Id.* at 7.

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”; 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.” *Id.* at 5-6.

Here, the AR confirms that DOJ has stockpiled millions of Americans’ confidential SVRL data for the first time, significantly changing a system of records long-maintained at CRT titled “JUSTICE/CRT – 001, Central Civil Rights Division Index File and Associated Records” (“Central CRT Index File”). *See, e.g.*, CRT-0004, -0024, -0031, -2057; *see also* CRT-3396 (acknowledging CRT ingesting “large datasets with PII” that “may potentially introduce new information types or require processing information in new ways,” including “[i]ngestion” and

“[s]torage of bulk confidential Voter Registration Data from multiple states”). DOJ has cited three pertinent SORNs for that system: 68 Fed. Reg. 47610 (Aug. 11, 2003), 70 Fed. Reg. 43904 (July 29, 2005), and 82 Fed. Reg. 24147 (May 25, 2017) (collectively, the “CRT SORNs”). *See* CRT-0004, -0024, -0031, -2057; Hill Decl. Exs. 10-12 (CRT SORNs). But none of the CRT SORNs—or any other—contemplates or discloses that the system will contain hundreds of millions of Americans’ SVRL data, that DOJ plans to disclose this sensitive personal data in bulk to other agencies and private contractors, and that DOJ plans to send the results of its “verification procedures” to states with instructions to remove purported “ineligible voters” DOJ identifies from their voter rolls. CRT-0005, 0007; CRT-0025, 0027; CRT-2058, 2060.

“[N]one of the SORNs” for the Central CRT Index File put the “American public on notice that specifically, their voter registration data is going to be collected [by DOJ] on an unprecedented level and used for a plethora of government activity . . . as required under the Privacy Act.” *Weber*, 816 F. Supp. 3d at 1193-94. The primary SORN, published in 2003, describes the system as consisting of “case files, matters, memoranda, correspondence, studies, and reports relating to enforcement of civil rights laws and other various duties of the Civil Rights Division.” Hill Decl. Ex. 10 (68 Fed. Reg. at 47611). But nothing in this or any CRT SORN notify the American public that the system will be used to retain, analyze, and disclose their personal state-level voter registration data en masse for DOJ’s secretive “list maintenance verification procedures.” CRT-0007 (Alaska MOU), CRT-0027 (South Carolina MOU), CRT-2060 (Texas MOU). For example, the CRT SORNs do not include registered voters in the “categories of individuals covered by the system,” do not include state voter registration data (let alone states’ entire SVRLs) in the “categories of records in the system,” and do not identify “list maintenance verification” as one of

the system's "purposes." *See* Hill Decl. Ex. 10 (68 Fed. Reg. at 47611); Hill Decl. Ex. 11 (70 Fed. Reg. 43904) (adding a routine use); Hill Decl. Ex. 12 (82 Fed. Reg. 24147) (adding routine uses).

Thus, as one court held in dismissing DOJ's voter data demand suit against California, DOJ has "violated" the Privacy Act's notice-and-comment requirements in compiling vast troves of new voter data in the Central CRT Index File. *See Weber*, 816 F. Supp. 3d at 1192-94. This subverts the "Privacy Act's public notice and comment structure," which "is an essential component of the Act and an essential piece of American democracy. Americans deserve to know the nature, scope, and routine uses of the records *before* they are collected by the federal government." *Id.* at 1193 (emphasis added). "If millions of Americans' private information is to be collected by the federal government, they deserve the ability to comment and voice their concerns before this collection occurs." *Id.*; *accord LULAC II*, 818 F. Supp. 3d at 113-15; OMB Privacy Act Guidelines, 40 Fed. Reg. 28948, 28966 (July 9, 1975), <https://perma.cc/776J-4L46>.

2. DOJ is improperly disclosing records in bulk in violation of the Privacy Act

Under the Voter List Maintenance Policy, DOJ is also violating the Privacy Act's prohibition on disclosures of individuals' records without their consent or statutory authorization, *see* Compl. ¶¶ 196-98, and thus has acted "not in accordance with law." 5 U.S.C. § 706(2)(A).

"An agency violates the [Privacy] Act when it 'discloses' information in the form of a 'record' from a 'system of records' and the disclosure is not pursuant to a valid exception under the Act." *Chichakli v. Tillerson*, 882 F.3d 229, 233 (D.C. Cir. 2018) (citing 5 U.S.C. § 552a(b)). Here, none of the Act's 13 exceptions apply, and DOJ's assertions to the contrary are meritless.

DOJ invokes the Act's "routine use" exception, *see, e.g.*, CRT-0004, -0024, -0031, which permits disclosure pursuant to a properly noticed "routine use," 5 U.S.C. § 552a(b)(3). "To fit within the confines of the routine use exception to the Privacy Act, an agency's disclosure of a

record must be both (i) ‘for a purpose which is compatible with the purpose for which it was collected’ and (ii) within the scope of a routine use notice published by the agency.” *Ames v. DHS*, 861 F.3d 238, 240 (D.C. Cir. 2017) (quoting 5 U.S.C. § 552a(a)(7) and citing § 552a(e)(4)(D)). As OMB’s guidelines instruct, “[a]gencies may only establish routine uses for a system by explicitly publishing the routine uses *in the relevant SORN*.” OMB Circular No. A-108 at 11 (emphasis added). Where, as here, old routine uses in outdated SORNs “do not accurately and completely describe all routine use disclosures to which the records in the system are subject, the agency *shall* discontinue any disclosures that are not accurately and completely described and revise the routine uses in the SORN to accurately and completely describe those disclosures.” *Id.* at 12 (emphasis added).

DOJ is defying this command. Pursuant to its Voter List Maintenance Policy, DOJ has executed agreements and policies freely allowing mass disclosure of SVRL data from the Central CRT File Index, in bulk, to persons within the agency, to DHS and other federal agencies, and to private contractors, as well as allowing DOJ to send its analysis of the SVRLs back to states. *See supra* Background §§ I.C-E. Yet, it is doing so under decades-old, outdated SORNs.

Nor do DOJ’s disclosures to DHS—whether to USCIS or HSI—fit the Privacy Act’s narrow “law enforcement” exception. That exception allows disclosure to another government agency “for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency . . . has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.” 5 U.S.C. § 552a(b)(7). The AR contains only one “written request” executed under (b)(7), under which U.S. Immigrations and Customs Enforcement (“ICE”) broadly requested that DOJ “provide HSI with the public [SVRLs] in its possession, in order for HSI to conduct appropriate

investigation of potential violations of federal election law.” CRT-3398. The letter failed to identify with any further specificity exactly what “potential violations of federal election law” ICE sought to investigate, *see id.*, falling short of even OLC’s assessment that, to satisfy the law enforcement exception, the letter “should specify that DHS seeks the [SVRLs] for the purpose of investigating violations of 18 U.S.C. §§ 611(a) and 1015(f), and specifically to identify illegal aliens who have registered to vote or have voted.” CRT-3368. The AR contains no written request from USCIS at all, as is required for DOJ to disclose voter data using SAVE.

And, in any case, 5 U.S.C. § 552a(b)(7) by its terms does not authorize the type of bulk, rolling data disclosures DOJ is making; it instead requires a targeted request specifying the “particular portion” of a record sought and “law enforcement activity” at issue. *Id.* This reading of (b)(7)’s plain text is confirmed by the Act’s legislative history. *See* S. Rep. No. 93-1183, at 70, 1974, U.S.C.C.A.N. at 6987 (recognizing that, in contrast to (b)(3)’s routine use exception, (b)(7)’s law enforcement exception allows “non-routine requests only where written requests and permission are given on a case-by-case basis by the agency maintaining the record”). Permitting the government to invoke the law enforcement exception to collect and query the voting records of hundreds of millions of Americans nationwide, without any individualized predicate, would allow the exception to swallow the rule and eviscerate the Privacy Act’s core protections.

By disclosing millions of Americans’ sensitive personal records with no applicable exception or properly noticed routine use, Defendants are violating 5 U.S.C. § 552a(b).

3. DOJ is maintaining inaccurate and outdated records in bulk in violation of the Privacy Act

Per the Policy, DOJ is maintaining inaccurate and outdated records in violation of the Privacy Act’s protections of individuals against adverse government determinations based on

faulty data. The Privacy Act requires agencies to ensure the records it “maintains”¹⁵ in systems of records are accurate, relevant, up-to-date, and secure. An agency must “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination,” 5 U.S.C. § 552a(e)(5); “make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes” before “disseminating” them “to any person other than a[] [federal] agency,” *id.* § 552a(e)(6); and “establish appropriate. . .safeguards . . . to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness,” *id.* § 552a(e)(10). DOJ is violating each of these restrictions by “maintaining” inaccurate, untimely, incomplete records in the Central CRT Index File to determine individuals’ eligibility to vote, without taking “reasonable efforts” to protect against the substantial risk DOJ will misidentify lawfully registered voters for purging.

As explained above, a key element of DOJ’s Voter List Maintenance Policy involves running millions of voters’ SVRL data through DHS’s SAVE system to conduct mass citizenship checks, and transmitting those results to states to mandate removal of individuals from voter rolls based on DOJ’s analyses. *See supra* Background §§ I.C-E. Yet the government itself admits—as reflected in the AR and other judicially noticeable federal records—that SAVE relies on incomplete and inaccurate citizenship data likely to falsely identify U.S. citizens as non-citizens or to fail to verify their citizenship. *See, e.g.*, CRT-0032 (acknowledging SAVE’s inability to

¹⁵ The Privacy Act defines “maintain” as “maintain, collect, use, or disseminate,” 5 U.S.C. § 552a(a)(3).

verify certain “acquired U.S. citizens”); Hill Decl. Exs. 13-15, 17 (DHS-AR-240, finding “risk” that SAVE “may share inaccurate information with registered agencies”); (DHS-AR-260, recognizing SAVE’s “[s]hortfalls in data accuracy”); (DHS-AR-302, stating same); (SSA-AR-44, stating “citizenship information in SSA’s records might not be current”); *see also League of Women Voters v. DHS*, 2025 WL 3198960, at *8 (D.D.C. Nov. 17, 2025) (“The Government does not dispute that . . . inaccuracies” in the SSA citizenship data used by SAVE “likely still exist.”). These data inaccuracies are known to cause “substantial harm, embarrassment, inconvenience, or unfairness,” *id.* § 552a(e)(10), to individuals wrongfully identified as non-citizens or potential non-citizens, including the Voter Plaintiffs and other Common Cause members. *See supra* Argument § I.

Moreover, DOJ acknowledges that states “update[]” SVRLs “regularly with new voter registrations,” and thus “the VRLs sent to [DOJ] won’t be current for very long – with updates, they will become obsolete.” CRT-3385. By DOJ’s own admission, then, the SVRL data it is maintaining, using, and disseminating will quickly become untimely and inaccurate.

By ingesting vast volumes of unreliable data in the Central CRT Index File and disclosing that data in bulk as part of DOJ’s Voter List Maintenance Policy, without protecting against known and substantial risks of “unfairness” in “determination[s],” *see* 5 U.S.C. §§ 552a(e)(5), (6), and (10), DOJ acted “not in accordance with law,” *id.* § 706(2)(A).

4. DOJ is maintaining First Amendment protected records in bulk in violation of the Privacy Act

DOJ is also violating the Privacy Act’s substantive restrictions by “maintaining” records in the Central CRT Index File that “describ[e] how an individual exercises rights guaranteed by the First Amendment,” even though such maintenance is not “expressly authorized by statute or by the individual about whom the record is maintained” and not “pertinent to and within the scope

of an authorized law enforcement activity.” 5 U.S.C. § 552a(e)(7); *see Weber*, 816 F. Supp. 3d at 1193 (holding that § 552a(e)(7) barred “DOJ’s request for California’s unredacted voter roll”). DOJ’s unprecedented “centralization” of millions of Americans’ First Amendment protected voting data has had and will have a profound “chilling effect on voter registration which would inevitably lead to decreasing voter turnout as voters fear that their information is being used for some inappropriate or unlawful purpose.” *Id.* at 1195-96.

First, DOJ is “maintaining” SVRLs in every sense of the statutory definition. *See* 5 U.S.C. § 552a(a)(3). DOJ “collected” the SVRLs from each Complying State. It “maintains” the SVRL data in the Central CRT Index File. It “uses” the SVRLs to conduct voter list verification and identify purportedly ineligible voters. And it “disseminates” the SVRLs to DHS and others to carry out DOJ’s list maintenance verification procedures. *See* CRT-0005, 0007 (Alaska MOU); CRT-0025, 0027 (South Carolina MOU); CRT-2058, 2060 (Texas MOU); *see also* CRT-0030-0040 (SAVE MOA between USCIS and DOJ); CRT-0003399-3400 (Agreement between HSI and DOJ); CRT-3396 (internal DOJ email describing “[p]otential analysis of ingested data by litigative consultant”).

Second, SVRLs are First Amendment protected records. “[V]oter registration, participation in elections, as well as party affiliation are all types of political expression protected by the First Amendment.” *Weber*, 816 F. Supp. 3d at 1193 (citing *Buckley v. Am. Const. L. Found., Inc.*, 525 U.S. 182, 195 (1999); *see also Rutan v. Republican Party of Ill.*, 497 U.S. 62, 69, 75-76 (1990)); *see also Gerlich v. DOJ*, 711 F.3d 161, 172 (D.C. Cir. 2013) (agency’s collection of records about individuals’ “ideological affiliations,” “political party affiliations,” or “involve[ment] in organizations committed to [partisan] causes” could violate § 552a(e)(7)). Because every SVRL reflects individuals’ registration to vote, SVRLs necessarily document First Amendment activity.

And some of the SVRLs that DOJ has compiled in the Central CRT Index File include even more details about individuals' First Amendment expression, including voter participation history and party affiliation. *See, e.g.*, CRT-0468, CRT-0947, CRT-1661, CRT-1843, CRT-1970.

Third, “none of the exceptions that would allow for agencies to collect information falling under the First Amendment apply in the present case.” *Weber*, 816 F. Supp. 3d at 1193. DOJ’s maintenance of the SVRL data is not “expressly authorized by statute,” 5 U.S.C. § 552a(e)(7), for the reasons explained above. *See supra* Argument § III.A. Nor is DOJ’s maintenance of First Amendment protected data pursuant to the Voter List Maintenance Policy “pertinent to and within the scope of an authorized law enforcement activity.” 5 U.S.C. § 552a(e)(7). DOJ may not “invok[e] a need to maintain records for generic investigative and informative purposes” under its purported HAVA and NVRA authority. *Maydak v. United States*, 363 F.3d 512, 517 (D.C. Cir. 2004); *see also MacPherson v. IRS*, 803 F.2d 479, 482 (9th Cir. 1986) (“The ‘law enforcement activities’ exception to the First Amendment protections of section (e)(7) of the Privacy Act is intended merely ‘to make certain that political and religious activities are not used as a cover for subversive activities.’”) (citing 120 Cong. Rec. H10, 892 (daily ed. Nov. 20, 1974)).

C. DOJ’s Voter List Maintenance Policy violates the Paperwork Reduction Act (Count VII)

As part of its Voter List Maintenance Policy, DOJ has demanded SVRLs without complying with the Paperwork Reduction Act’s procedural requirements and thus acted “without observance of procedure required by law.” 5 U.S.C. § 706(2)(D).¹⁶

¹⁶ An agency’s failure to adhere to PRA procedures is appropriately enforced through the APA. *See, e.g., Hyatt v. OMB*, 908 F.3d 1165, 1172-73 (9th. Cir. 2018); *Doctors for America v. OPM*, 766 F. Supp. 3d 39, 52 (D.D.C. 2025); *Orr v. Trump*, 778 F. Supp. 3d 394, 425-26 (D. Mass. 2025).

“The PRA provides that agencies cannot ‘conduct or sponsor’ a ‘collection of information’ unless they comply with several procedural requirements.”¹⁷ *Hyatt*, 908 F.3d at 1171. *First*, the agency must conduct an extensive review of the proposed collection, including (among other things) evaluating “the need for the collection of information,” devising “a plan for the collection of information,” confirming that the “collection is in accordance with the clearance requirements” provided in the statute. *See* 44 U.S.C. §§ 3506(c)(1) & 3507(a)(1). *Second*, the agency must post a 60-day notice in the Federal Register soliciting comments that allow it, *inter alia*, to “evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency.” *Id.* §§ 3506 (c)(2) & 3507(a)(2). *Third*, the agency must certify to the Director of the Office of Management and Budget (“OMB”) that the collection of information satisfies several statutory safeguards, including that it “informs the person receiving the collection of information of [] the reasons the information is being collected [and] the way such information is to be used.” *Id.* § 3506(c)(1)(B)(iii) & (c)(3). *Fourth*, it must publish a second detailed notice in the Federal Register. *Id.* § 3507(a)(1)(D). After this process, the agency may proceed with the collection of information *only* if the Director of OMB approves the collection and provides it with a “control number to be displayed upon the collection of information.” *Id.* § 3507(a)(2)-(3).¹⁸

¹⁷ A “collection of information” is defined broadly to include “the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of format, calling for either [*inter alia*] answers to identical questions posed to, or identical reporting . . . requirements imposed on [] ten or more persons.” 44 U.S.C. § 3502(3)(A). The term “person” is defined to include states. *Id.* § 3502(10).

¹⁸ The statute ensures that the OMB Director’s review imposes meaningful safeguards: it requires the Director, “[b]efore approving a proposed collection of information,” to make an independent determination of whether the collection is “necessary for the proper performance of the functions of the agency.” 44 U.S.C. § 3508. If the OMB Director “determines that the collection of information . . . is unnecessary for any reason, the agency may not engage in the collection of information.” *Id.*

DOJ's demand letters violated each of these clear statutory requirements, and therefore violated the PRA. To start, the demand letters constitute a "collection of information" under the statute. To trigger the statute's requirements, a collection of information must pose "identical questions . . . or reporting requirements" directed to "ten or more persons." 44 U.S.C. § 3502(3)(A). The demand letters satisfy that requirement: DOJ sent demands to 49 states and the District of Columbia, and each demanded "all fields" contained in the state's SVRL, including "the registrant's full name, date of birth, residential address, his or her state driver's license number, or the last four digits of the registrant's social security number." *See supra* note 7.¹⁹ DOJ was therefore subject to the PRA's procedural requirements, yet it ignored them. The letters did not display OMB-issued control numbers, and they could not have, because DOJ did not comply with any of the Act's enumerated procedures.

DOJ's demand for sensitive data about hundreds of millions of Americans is exactly the kind of governmental action that the PRA is meant to regulate. Passed in response to the federal government's "insatiable appetite for data," the PRA requires agencies to observe "procedures for guarding the privacy" of individuals when the government seeks their "confidential information." *Dole v. United Steelworkers of Am.*, 494 U.S. 26, 32 (1990). When it enacted the PRA in 1980, Congress declared its intent (among other things) to "ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the federal Government is consistent with applicable law, including laws relating to [] privacy and confidentiality, including [the Privacy Act]." 44 U.S.C. § 3501(8)(A). If DOJ had adhered to the PRA's procedures, it would have had to consider the legal and practical consequences of amassing a

¹⁹ The PRA applies to collections of information directed to state governments or their officials. *See* 42 U.S.C. § 3502(10).

national voter registration database. Flouting the statute’s procedures thus undermines the exact interests Congress sought to protect.²⁰

D. DOJ’s Policy is arbitrary and capricious (Count VIII)

DOJ’s sweeping Policy—requiring states to surrender their complete confidential voter list data to the federal government, issued without formal rulemaking or even a written memorandum of decision—is also arbitrary and capricious and must be set aside on that basis. 5 U.S.C. § 706(2)(A). The APA “requires agencies to engage in reasoned decisionmaking” and “to reasonably explain to reviewing courts the bases for the actions they take and the conclusions they reach.” *Bhd. of Locomotive Eng’rs & Trainmen v. Fed. R.R. Admin.*, 972 F.3d 83, 115 (D.C. Cir. 2020) (quoting *DHS v. Regents of the Univ. of Cal.*, 591 U.S. 1, 16 (2020)). DOJ has failed to meet this foundational requirement, as shown by the certified AR containing all “materials that might have influenced the agency’s decision” in establishing the Policy. *See Amfac Resorts v. U.S. Dep’t of the Interior*, 143 F. Supp. 2d 7, 12 (D.D.C. 2001) (citation modified). The AR establishes that Defendants have failed to explain the Policy; the Policy decision runs counter to the evidence before the agency; DOJ “entirely failed to consider [] important aspect[s] of the problem;” and it has “relied on factors which Congress has not intended it to consider.” *Motor Vehicle Mfrs. Ass’n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983). The Policy is arbitrary and capricious for each of these independent reasons.

²⁰ DOJ may seek to defend its overt defiance of the PRA’s procedural requirements by invoking the exception for requests tied to litigation or administrative enforcement, 44 U.S.C. § 3518(c)(1), but any such argument lacks merit. The PRA specifically *includes* within its scope collections of information in pursuit of “general investigations.” *Id.* § 3518(c)(2). DOJ’s categorical, nationwide demand for SVRL data epitomizes a “general investigation.”

1. Defendants failed to explain the Policy

The D.C. Circuit has repeatedly held that “a fundamental requirement of administrative law is that an agency set forth its reasons for decision; an agency’s failure to do so constitutes arbitrary and capricious agency action.” *Amerijet Int’l, Inc. v. Pistole*, 753 F.3d 1343, 1350 (D.C. Cir. 2014) (cleaned up). Notwithstanding the magnitude of DOJ’s Policy – affecting hundreds of millions of voters nationwide – it has not explained its Policy to compile the states’ confidential voter files, let alone a reasoned one. The absence of a reasoned explanation for the agency’s decision renders it arbitrary and capricious and requires the Court to set it aside. *See FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 513 (2009) (“we insist that an agency ‘examine the relevant data and articulate a satisfactory explanation for its action.’”) (citation omitted).

The “reasoned explanation requirement . . . is meant to ensure that agencies offer genuine justifications for important decisions, reasons that can be scrutinized by courts and the interested public.” *Dep’t of Com.*, 588 U.S. at, 756. The Policy fails to meet the most fundamental APA requirement that an agency engage in reasoned decisionmaking and must be set aside for this reason alone.

2. DOJ failed to explain a rational connection between the facts and the Policy

An “agency’s substantive decision must be supported by ‘substantial evidence’ in the administrative record.” *Nat’l Lifeline Ass’n v. Fed. Commc’ns Comm’n*, 921 F.3d 1102, 1111 (D.C. Cir. 2019) (quoting *Comcast Corp. v. FCC*, 579 F.3d 1, 5, 7 (D.C. Cir. 2009)). The AR confirms that DOJ fails to meet this independent requirement of reasoned decisionmaking, as DOJ failed to conduct or even consult any research or analysis *before* implementing this nationwide Policy. *See generally* AR.

Although Defendants' MOUs with states include conclusory references to Title III of the CRA, HAVA, and the NVRA, *see, e.g.*, CRT-0001, CRT-0017, neither the MOUs nor any other Record document includes any explanation for how these statutes relate to Defendants' data demands.²¹ *See generally* AR. The PRA required DOJ to articulate precisely this kind of reasoning before launching a collection of information. *See supra* Argument § III.C. DOJ's "failure to comply with, or apparently even consider, the PRA also lends support for Plaintiffs' argument that the [Voter List Maintenance Policy] is arbitrary and capricious." *Am. Fed'n of Tchrs. v. Dep't of Educ.*, 796 F. Supp. 3d 66, 103 (D. Md. 2025).

3. DOJ entirely failed to consider important aspects of the problem

In its decision-making process, DOJ "entirely failed to consider [] important aspect[s] of the problem," *State Farm*, 463 U.S. at 43, including voter participation and disenfranchisement, personal data privacy, and data security. This is an independent basis to set aside the Policy under the APA. *See Nat'l Lifeline Ass'n*, 921 F.3d at 1113 (vacating agency action for failing to consider its effects on impacted groups).

First, the AR is silent on the privacy and cybersecurity risks associated with compiling, centralizing, and sharing the personal data of over 200 million active registered voters. *See generally* AR. The AR contains no notice published in the Federal Register, no privacy impact assessment, no privacy threshold analysis, and no explanation of what measures, if any, Defendants are taking to ensure the data will be maintained with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the

²¹ Post hoc rationalizations suggest that DOJ may seek to justify its Policy by reference to claims of election fraud, voter list maintenance errors, or civil rights violations. *See, e.g.*, CRT-0001 (Alaska MOU); CRT-0017 (South Carolina MOU). However, a court may not accept "post hoc rationalizations for agency action." *State Farm*, 463 U.S. at 50. "It is well-established that an agency's action must be upheld, if at all, on the basis articulated by the agency itself." *Id.*

determination.” 5 U.S.C. § 552a(e)(5). *See also generally* AR. A “statutorily mandated factor, by definition, is an important aspect of any issue before an administrative agency, as it is for Congress in the first instance to define the appropriate scope of an agency’s mission.” *Pub. Citizen v. Fed. Motor Carrier Safety Admin.*, 374 F.3d 1209, 1216 (D.C. Cir. 2004).

Defendants also failed to consider the substantial risk that the Policy would result in the erroneous removal of eligible voters from states’ SVRLs. After Defendants adopted the Policy, they expressed awareness that SAVE *cannot* identify certain eligible voters, namely citizens with acquired citizenship, CRT-0032 n.2. DHS itself has repeatedly confirmed these risks. *See supra* Background § I.D. Critically, the AR confirms that Defendants did not consider any of these risks *before* the Policy was developed and implemented. This alone is evidence of arbitrary and capricious decision-making in violation of the APA. *See Council of Parent Att’ys & Advocs., Inc. v. DeVos*, 365 F. Supp. 3d 28, 54 (D.D.C. 2019) (vacating arbitrary and capricious agency action when “the government failed to adequately account for two relevant factors—the States’ reliance cost and the cost of delay on children, parents, and society”).

DOJ further failed to consider the reliance interests and reasonable privacy expectations of the millions of Americans who never consented to their voter data being compiled, consolidated, analyzed, and shared by DOJ. *See generally* AR. *See Nat’l Lifeline Ass’n*, 921 F.3d at 1114-15 (failing to consider reliance interests was arbitrary and capricious). Plaintiff Common Cause has relied on its knowledge of longstanding government practices and information disclosed under open government laws to educate and inform the public to achieve its mission of protecting fair and equal access to the ballot box. *See* Nunez Decl. ¶¶ 20, 22. DOJ’s Policy ignores those reliance interests, leaving Common Cause and similar organizations in the dark as to how to educate the public about the security of voter data and how the federal government will use voters’ sensitive

information. *See generally* AR. When an agency’s “prior policy has engendered serious reliance interests that must be taken into account.” *Fox Television Stations*, 556 U.S. at 515. “It would be arbitrary or capricious to ignore such matters.” *Id.* DOJ’s failure to even acknowledge the “serious reliance interests” at issue is arbitrary and capricious, as “a reasoned explanation is needed for disregarding facts and circumstances that underlay or were engendered by the prior policy.” *Id.* at 516.

Finally, the Policy is antithetical to Congress’s goals in enacting the NVRA. As DOJ itself acknowledges, Congress’s intent in enacting the NVRA was to make “it easier for all Americans to register to vote and to maintain their registration.”²² “Congress’s stated purposes in enacting the NVRA included ‘establish[ing] procedures that will increase the number of eligible citizens who register to vote in elections for Federal office,’ helping officials at all levels of government implement the Act’s requirements ‘in a manner that enhances the participation of eligible citizens as voters in elections for federal office,’ ‘protect[ing] the integrity of the electoral process,’ and ensuring the maintenance of ‘accurate and correct voter registration rolls.’” *LULAC II*, 818 F. Supp. 3d at 62 (citations omitted). By increasing the likelihood that eligible voters will be erroneously removed from states’ voter rolls, the Policy offends each of Congress’s purposes. *See, e.g.*, CRT-0032 (SAVE MOA between USCIS and DOJ) (“SAVE may only be able to verify acquired U.S. citizenship in certain situations,” and if DOJ queries “an individual with acquired citizenship who has not applied for a Certificate of Citizenship with [DHS], . . . SAVE may not be able to confirm that individual’s acquired citizenship.”).

²² DOJ Civil Rights Division, *About The National Voter Registration Act*, <https://www.justice.gov/crt/about-national-voter-registration-act>.

Defendants’ “decision to disregard” each of these crucial concerns when developing its policy involving the collection, maintenance, sharing, and alteration of states’ confidential voter lists was “arbitrary and capricious.” *Pub. Emps. for Env’t Resp. v. Hopper*, 827 F.3d 1077, 1090 (D.C. Cir. 2016); accord *Carlson v. Postal Regul. Comm’n*, 938 F.3d 337, 344 (D.C. Cir. 2019); *Sierra Club v. Dep’t of Transp.*, 125 F.4th 1170, 1182 (D.C. Cir. 2025). Ultimately, having conducted no factfinding or analysis and provided no explanation in developing the Policy, Defendants “acted essentially as a rubber stamp” for the administration’s directives to federalize voter list maintenance. *Sierra Club v. Salazar*, 177 F. Supp. 3d 512, 541 (D.D.C. 2016). The Policy is arbitrary and capricious for this independent reason.

IV. Plaintiffs are entitled to their requested relief

Plaintiffs respectfully request vacatur of the Policy, rescission of the actions taken pursuant to the Policy, and injunctive and declaratory relief.

A. The Court should set aside and vacate the Policy under the APA

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, unconstitutional, arbitrary and capricious, or procedurally defective. 5 U.S.C. § 706(2)(A)-(D). Here, if the Court finds that Plaintiffs have prevailed on any of one or more of the APA claims relevant to this motion (Counts I, VI, VII, and VIII), the Court “shall” apply this default rule and set aside Defendants’ Policy. “[T]o ‘set aside’” an agency action “is to vacate it.” *Bridgeport Hosp. v. Becerra*, 108 F.4th 882, 890 (D.C. Cir. 2024). See also *Allina Health Servs. v. Sebelius*, 746 F.3d 1102, 1110 (D.C. Cir. 2014) (“vacatur is the normal remedy” for an APA violation).

The goal of vacatur is to “re-establish the status quo absent the unlawful agency action.” *Las Ams. Immigrant Advoc. Ctr. v. DHS*, 783 F. Supp. 200, 233 (D.D.C. 2025). Here, vacatur requires DOJ to set aside the Policy and cease all actions to compile, consolidate, disclose,

compare, and analyze SVRL data; withdraw all associated policies and agreements; delete, disentangle, and unlink any SVRL data DOJ has in its possession, custody, or control; and instruct any governmental or nongovernmental third party that has received SVRL data as a result of the Policy to delete, disentangle, and unlink all such data. Such relief is necessary to “re-establish the status quo absent the unlawful agency action,” *id.*, and consistent with relief courts have found appropriate in APA cases. *See, e.g., Massachusetts v. Dep’t of Educ.*, --- F. Supp. 3d ---, No. 26-cv-11229, 2026 WL 918941, at *19 (D. Mass. Apr. 3, 2026) (granting preliminary injunction and separately ordering the Department of Education to cease collecting data pending trial on the merits, *see* ECF 143 for order). Vacatur is also the “ordinary” remedy for procedural APA violations based on failures to follow statutory “notice-and-comment requirements.” *City of Billings v. TSA*, 153 F.4th 46, 54 (D.C. Cir. 2025); *accord Daimler Trucks N. Am. LLC v. EPA*, 737 F.3d 95, 103 (D.C. Cir. 2013) (courts “typically vacate[] rules when an agency ‘entirely fail[s]’ to provide notice and comment” (citation omitted)).

B. Alternatively, the Court should permanently enjoin the Voter List Maintenance Policy

In the alternative, if the Court finds vacatur alone does not encompass Plaintiffs’ requested relief, the APA also authorizes the Court to issue “writs of prohibitory or mandatory injunction.” 5 U.S.C. § 703. A district court vacating an agency action under the APA may issue an injunction where doing so would “‘have [a] meaningful practical effect independent of its vacatur.’” *N. Am. ’s Bldg. Trades Unions v. Dep’t of Def.*, 783 F. Supp. 3d 290, 312 (D.D.C. 2025) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 165 (2010)). Under these principles, this Court may supplement vacatur with injunctive relief as necessary to fully remedy Plaintiffs’ injuries. Thus, to the extent such relief is not encompassed within vacatur, Plaintiffs request a permanent injunction (1) prohibiting DOJ’s actions to compile, consolidate, disclose, compare, and analyze SVRL data

pursuant to the Voter List Maintenance Policy; (2) ordering DOJ to withdraw all associated policies and agreements; and (3) ordering DOJ to delete, disentangle, and unlink any SVRL data it has in its possession, custody, or control and instruct any governmental or nongovernmental third party that has received SVRL data as a result of the Policy to do the same.²³

Such a remedy is necessary to fully redress Plaintiffs' injuries because, as discussed above, *supra* Argument § I, those ongoing injuries stem from the misappropriation of sensitive voter records. When an improper disclosure of sensitive information occurs in violation of statute or the Constitution, a court can remedy the ongoing injury resulting from "the Government's continued possession of those materials." *Cf. Church of Scientology of Cal. v. United States*, 506 U.S. 9, 12-13 (1992). "Even though it is now too late to prevent, or to provide a fully satisfactory remedy for, the invasion of privacy that occurred . . . a court does have the power to effectuate a partial remedy by ordering the Government to destroy . . . any and all copies it may have in its possession." *Id.*; *see also AFSCME*, 172 F.4th at 373 (observing that permanent injunction "order[ing] the relevant employees to destroy any illegally obtained data or work derived from such data" would be appropriate remedy for unlawful disclosure); *Chastain v. Kelley*, 510 F.2d 1232, 1235 (D.C. Cir. 1975) ("The federal courts are empowered to order the expungement of Government records where necessary to vindicate rights secured by the Constitution or by statute.").

²³ DOJ's Policy will "irreparably harm Plaintiffs' 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 II*, 818 F. Supp. 3d at 102. Specifically, Common Cause will lose the opportunity to use its limited resources to educate and register more voters in furtherance of its mission, and its members, including the Voter Plaintiffs, could lose their right to vote or face significant hurdles to voting. *See supra* Argument § I. 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 a permanent injunction." *LULAC II*, 818 F. Supp. 3d at 102 (quoting *Newby*, 838 F.3d at 9).

The permanent injunction Plaintiffs seek is also necessary to afford them complete relief. Because Common Cause is a national organization with nearly one million members and a presence in all fifty states and the District of Columbia, *see* Nunez Decl. ¶¶ 5, 7, enjoining DOJ from collection, maintenance, and disclosure of SVRL data and requiring DOJ to delete the existing data in its possession, custody, and control is a party-specific remedy. *See LULAC I*, 808 F. Supp. 3d at 85 (holding that because organizational plaintiffs operated and had members nationwide, a national injunction “is a remedy that is ‘specific’ to the Plaintiffs because no other remedy would afford complete relief.”) (citation omitted). Additionally, Plaintiffs’ challenge “do[es] not involve the case-by-case enforcement” of the policy but rather concerns the Policy in its entirety. *Id.*

C. The Court should declare the Policy unlawful

Plaintiffs also seek a declaratory judgment that DOJ’s Policy and all associated policies and agreements are unlawful. These are issues of unquestionable public importance, particularly given looming nationwide elections. Such declaratory relief will both “serve a useful purpose in clarifying the legal relations at issue” and “afford relief from the uncertainty, insecurity, and controversy giving rise to the proceeding.” *President v. Vance*, 627 F.3d 353, 364 n.76 (D.C. Cir. 1980) (citations omitted). A declaratory judgment is warranted here for each independent reason. *See LULAC II*, 818 F. Supp. 3d at 90-91. *Cf. Newby*, 838 F.3d at 13 (“Confusion will create a disincentive for citizens who would otherwise attempt to register to vote” (citing *Purcell*, 549 U.S. at 4-5)).

CONCLUSION

The Court should grant Plaintiffs’ motion for partial summary judgment.

Dated: May 19, 2026

Respectfully submitted,

/s/ Nikhel S. Sus

Nikhel S. Sus (D.C. Bar No. 1017937)

John B. Hill (N.Y. Bar No. 5505508)*

CITIZENS FOR RESPONSIBILITY

AND ETHICS IN WASHINGTON

P.O. Box 14596

Washington, DC 20044

Tel: (202) 408-5565

nsus@citizensforethics.org

jhill@citizensforethics.org

Sara Chimene-Weiss*

PROTECT DEMOCRACY PROJECT

7000 N. 16th Street, Suite 120, #340

Phoenix, AZ 85020

Tel: (202) 934-4237

sara.chimene-weiss@protectdemocracy.org

Jane Bentrrott (D.C. Bar No. 1029681)

Naomi Gilens (D.C. Bar No. 90037831)

PROTECT DEMOCRACY PROJECT

2020 Pennsylvania Ave. NW, Suite #163

Washington DC 20006

Tel: (202) 579-4582

jane.bentrrott@protectdemocracy.org

naomi.gilens@protectdemocracy.org

Jared Fletcher Davidson*

PROTECT DEMOCRACY PROJECT

82 Nassau Street, #601

New York, NY 10038

Tel: (202) 579-4582

jared.davidson@protectdemocracy.org

John Haubenreich*

PROTECT DEMOCRACY PROJECT

1108 McKennie Ave., Suite #223

Nashville, TN 37206

Tel: (202) 579-4582

john.haubenreich@protectdemocracy.org

Laurence M. Schwartztol (D.D.C. Bar No. MA0007)

DEMOCRACY AND RULE OF LAW CLINIC,

HARVARD LAW SCHOOL

1525 Massachusetts Avenue
Cambridge, MA 02138
Tel: (617) 998-1877
lschwartztol@law.harvard.edu

Ming Cheung*
Ari J. Savitzky*
Theresa J. Lee*
Sophia Lin Lakin*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Tel: (212) 549-2500
mcheung@aclu.org
asavitzky@aclu.org
tle@aclu.org
slakin@aclu.org

Laura K. Follansbee (D.C. Bar No. 1782046)
Arthur B. Spitzer (D.C. Bar No. 235960)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF THE DISTRICT OF COLUMBIA
529 14th Street NW, Suite 722
Washington, DC 20045
Tel: (202) 457-0800
lfollansbee@acludc.org
aspitzer@acludc.org

* Admitted *pro hac vice*

Counsel for Plaintiffs

Exhibit A

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

vs.

Case No. 1:26-cv-01352-SLS

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

DECLARATION OF JOHN B. HILL

I, John B. Hill, declare as follows:

1. I am Senior Litigation Counsel at Citizens for Responsibility and Ethics in Washington (“CREW”) and counsel for Plaintiffs in the above-captioned action.

2. In a February 2, 2026, interview on the Dan Bongino Show, President Trump said “[t]he Republicans should say we want to take over, we should take over the voting, and at least many, 15 places the Republicans ought to nationalize the voting.” A true and correct video of that interview is available here: <https://vimeo.com/1161365870>, at 14:24.

3. In a February 3, 2026, press conference, President Trump was asked “Mr. President, what exactly did you mean when you said that you should nationalize elections?” President Trump responded “I want to see elections be honest. And if a state can’t run an election, I think the people behind me should do something about it because, you know, if you think about it, a state is an agent for the federal government in elections. I don’t know why the federal government doesn’t do them anyway.” A true and correct video of that press conference is available here: <https://www.youtube.com/watch?v=xcEw3TCktIw>.

4. A true and correct copy of the following article, Erica L. Green, Michael Gold & Robert Jimison, *Trump Repeats Call to 'Nationalize' Elections, as White House Walks It Back*, N.Y. Times (Feb. 3, 2026), is available here

<https://www.nytimes.com/2026/02/03/us/politics/trump-save-act-elections.html> and attached hereto as Exhibit 1.

5. A true and correct copy of an August 18, 2025, Truth Social post from the account @realDonaldTrump is available here

<https://truthsocial.com/@realDonaldTrump/posts/115049485680941254> and attached hereto as Exhibit 2.

6. A true and correct copy of Executive Order No. 14399, Ensuring Citizenship Verification and Integrity in Federal Elections, 91 Fed. Reg. 17125 (Mar. 31, 2026), is available here <https://www.govinfo.gov/content/pkg/FR-2026-04-03/pdf/2026-06601.pdf> and attached hereto as Exhibit 3.

7. A true and correct copy of Executive Order No. 14248, Preserving and Protecting the Integrity of American Elections, 90 Fed. Reg. 14005 (Mar. 25, 2025), is available here <https://www.govinfo.gov/content/pkg/FR-2025-03-28/pdf/2025-05523.pdf> and attached hereto as Exhibit 4.

8. On April 19, 2026, U.S. Department of Justice (“DOJ”) Assistant Attorney General for Civil Rights Harmeet Dhillon appeared on FOX News. A true and correct video of that appearance is available here: <https://www.youtube.com/watch?v=3eJVzgDj5TY>.

9. A true and correct copy of the relevant excerpts from a transcript of the March 26, 2026, hearing held in *United States v. Amore*, No. 25-cv-639 (D.R.I.), is attached hereto as Exhibit 5.

10. A true and correct copy of the relevant excerpts from a transcript of the March 19, 2026, hearing held in *United States v. Thomas*, No. 26-cv-00021, ECF No. 86 (D. Conn.), is attached hereto as Exhibit 6.

11. A true and correct copy of the Declaration of DOJ Acting Chief to the Voting Section within the Civil Rights Division Eric Neff, filed in *United States v. Galvin*, No. 25-cv-13816, ECF No. 70-2 (D. Mass. Feb. 27, 2026) is available here <https://storage.courtlistener.com/recap/gov.uscourts.mad.293151/gov.uscourts.mad.293151.70.2.pdf> and attached hereto as Exhibit 7.

12. A true and correct copy of the following article, Abby Vesoulis & Ari Berman, *Your Private Data Is Building Trump's Voter Purge Machine*, Mother Jones (Dec. 5, 2025), <https://www.motherjones.com/politics/2025/12/your-private-data-is-building-trumps-voter-purge-machine/> is attached hereto as Exhibit 8.

13. On March 17, 2026, Assistant Attorney General for Civil Rights at DOJ Harmeet Dhillon appeared on Newsmax. A true and correct video of that appearance is available here: https://www.youtube.com/watch?v=132KPr2_FBk.

14. A true and correct copy of a February 11, 2026, Letter from Office of Kris Warner, Sec'y of State of West Virginia, to Eric Neff, Acting Chief of the Civil Rights Division Voting Section at DOJ, is available here <https://files.constantcontact.com/e949222d701/ed164568-7c31-48e6-a03f-89f082080313.pdf> and attached as Exhibit 9.

15. A true and correct copy of DOJ's System of Records Notice for Central Civil Rights Division Index File and Associated Records, JUSTICE/CRT-001, 68 Fed. Reg. 47610 (August 11, 2003), is available here

<https://www.govinfo.gov/content/pkg/FR-2003-08-11/pdf/03-20342.pdf> and attached hereto as Exhibit 10.

16. A true and correct copy of DOJ's System of Records Notice for Central Civil Rights Division Index File and Associated Records, JUSTICE/CRT-001, 70 Fed. Reg. 43904 (July 29, 2005), is available here

<https://www.govinfo.gov/content/pkg/FR-2005-07-29/pdf/05-14944.pdf> and attached hereto as Exhibit 11.

17. A true and correct copy of DOJ's System of Records Notice for Central Civil Rights Division Index File and Associated Records, JUSTICE/CRT-001, 82 Fed. Reg. 24147 (May 25, 2017), is available here

<https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10780.pdf> and attached hereto as Exhibit 12.

18. I serve as counsel for Plaintiffs in *League of Women Voters v. DHS*, No. 25-cv-3501-SLS (D.D.C.). In that case, Defendants Department of Homeland Security and Social Security Administration produced the following documents as a part of the Administrative Record, a true and correct copy of which are attached hereto:

- DHS-AR-221-243 - DHS, Privacy Impact Assessment for the Systematic Alien Verification for Entitlements "SAVE" Program, DHS Reference No. DHS/USCIS/PIA-006(d) (Oct. 31, 2025) - attached as Exhibit 13;
- DHS-AR-244-85 - DHS-USCIS-PTA, SAVE Program Optimization Privacy Threshold Analysis (PTA) Final Adjudication (July 17, 2025) - attached as Exhibit 14;
- DHS-AR-286-327 - DHS-USCIS-PTA, SAVE Program Optimization Privacy Threshold Analysis (PTA) Final Adjudication (Sept. 11, 2025) - attached as Exhibit 15;
- DHS-AR-483-90 - USCIS, DHS, Narrative Statement for SORN Update, Submitted to DCPO (Feb. 2025) - attached as Exhibit 16;
- SSA-AR-30-49 - Department of the Treasury, Agreement Between Federal Program Agencies for Intragovernmental Reimbursable, Buy/Sell Activity, SSA-DHS-USCIS

(May 15, 2025) - attached as Exhibit 17; and

- SSA-AR-89-108 - Department of the Treasury, Agreement Between Federal Program Agencies for Intragovernmental Reimbursable, Buy/Sell Activity. SSA-DHS-USCIS (Aug. 2025) - attached as Exhibit 18.

19. A true and correct copy of a July 13, 2023, letter from the Social Security

Administration Office of General Counsel to Fair Elections Center is available here,

<https://fairelectionscenter.org/wp-content/uploads/2025/07/SSA-Touhy-Decision-letter.July-13-2023-signed.pdf> and attached hereto as Exhibit 19.

20. A true and correct copy of the December 18, 2006, *Congressional Response*

Report: Accuracy of the Social Security Administration's Numident File, No. A-08-06-26100,

from the Social Security Administration's Office of the Inspector General, is available here,

https://oig-files.ssa.gov/audits/full/A-08-06-26100_0.pdf and attached hereto as Exhibit 20.

21. On November 4, 2025, CREW submitted a Freedom of Information Act ("FOIA")

request to the U.S. Department of Justice's Civil Rights Division (the "FOIA Request"). CREW

requested the following categories of records beginning on January 20, 2025:

- All formal or information data sharing agreements between DOJ and any state or election official providing access to personally identifiable information ("PII");
- All records relating to DOJ's use of the Department of Homeland Security's Systematic Alien Verification for Entitlements ("SAVE") system for purposes of verifying the citizenship of voters or voter registrants in any state; and
- Agency records sufficient to show:
 - All formal or informal policies, determinations or conclusions (including underlying memoranda) concerning the scope of DOJ's use of the PII it seeks from election officials. This includes records reflecting any plans for how the agency will compile, aggregate, synthesize, match, link, or otherwise combine data obtained from an election official with any other data; and
 - Privacy or data security safeguards in place for protecting PII shared by election officials.

22. After the District Court for the District of Columbia entered a preliminary

injunction against DOJ ordering DOJ to expedite processing of the FOIA Request, DOJ produced, among other records, the following record at Bates number CREW v. DOJ - CRT - 1305, a true and correct copy of which is attached hereto as Exhibit 21.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 18, 2026, in Pennsylvania.



John B. Hill

Exhibit 1

Trump Repeats Call to ‘Nationalize’ Elections, as White House Walks It Back

President Trump’s extraordinary comments were the latest iteration of his unsubstantiated claims that U.S. elections are rigged as Republicans face potentially big losses this fall.

▶ Listen · 7:31 min



By Erica L. Green, Michael Gold and Robert Jimison

Reporting from Washington

Feb. 3, 2026

President Trump doubled down on his extraordinary call for the Republican Party to “nationalize” voting in the United States, even as the White House tried to walk it back and members of his own party criticized the idea.

Mr. Trump said on Tuesday that he believed the federal government should “get involved” in elections that are riddled with “corruption,” reiterating his position that the federal government should usurp state laws by exerting control over local elections.

If states “can’t count the votes legally and honestly, then somebody else should take over,” he said in the Oval Office, accusing several Democratic-run cities of corruption. “Look at some of the places — that horrible corruption on elections — and the federal government should not allow that,” he added. “The federal government should get involved.”

Mr. Trump's remarks came hours after the White House tried to walk back his comments from a day earlier that his party should nationalize elections. And they were the latest iteration of his unsubstantiated claims that U.S. elections are rigged, as Republicans face potentially big losses this fall.

During a podcast interview with Dan Bongino, his former deputy F.B.I. director, on Monday, Mr. Trump called for Republican officials to "take over" voting procedures in 15 states, though he did not name them. "The Republicans should say, 'We want to take over,'" he said. "We should take over the voting, the voting in at least many — 15 places. The Republicans ought to nationalize the voting."

Mr. Trump's statement amounted to a remarkable escalation of the president's attempt to exert power over the outcome of future elections. Under the Constitution, American elections are governed primarily by state law, leading to a decentralized process in which voting is administered by county and municipal officials in thousands of precincts across the country.

But Karoline Leavitt, the White House press secretary, said on Tuesday that Mr. Trump had actually been referring to legislation that would require people to prove that they are U.S. citizens when they register to vote.

"What the president was referring to is the SAVE Act, which is a huge, common-sense piece of legislation that Republicans have supported, that President Trump is committed to signing into law during his term," Ms. Leavitt said.

"I don't think any rational person who is being honest with themselves would disagree with the idea of requiring citizens of this country to present an ID before casting a ballot in a federal election, or, frankly, in any election, and that's something the president wants to see happen."

But Mr. Trump never referenced the SAVE Act during the podcast or in his appearance in the Oval Office on Tuesday. And in any case, the SAVE Act does not federalize elections.

Ms. Leavitt said that “the president believes in the United States Constitution,” but that he also believed there had been “a lot of fraud and irregularities that have taken place in American elections.”

Ms. Leavitt did not identify the 15 states Mr. Trump was referring to on the podcast. She cited only California and New York — two Democratic-led states the president often targets — as examples of places where noncitizens are allowed to vote in their elections, creating a situation she said was “ripe with fraud.”

Not long after Ms. Leavitt made her statement, Mr. Trump again spoke about federal control over elections.

“I want to see elections be honest, and if a state can’t run an election, I think the people behind me should do something about it,” Mr. Trump said in the Oval Office, where Republican lawmakers from both chambers of Congress joined him at the signing of legislation to end the partial government shutdown.

Mr. Trump’s comments and an intensifying Republican push in Congress to tighten voting laws — along with an F.B.I. move last week to seize ballots and other voting records from the 2020 election from an election center in Fulton County, Ga., — suggests a broader drive by the president and his allies to sow distrust of American elections ahead of midterm balloting in November.

Mr. Trump himself has repeatedly forecast in recent months that Republicans would lose midterms, after the party was rattled by losing several local races last November, and a Democrat won a special election in Texas last week in a district that Mr. Trump had won by double digits.

Voting by noncitizens happens rarely, and it is already illegal in federal elections. But Mr. Trump and many of his allies repeatedly and baselessly insisted during the 2024 election that noncitizens were flooding to the polls — a campaign of misinformation that has ramped up in recent weeks as the election nears.

The Justice Department, which has been newly politicized under Mr. Trump, is demanding that numerous states, including Minnesota, turn over their full voter rolls as the Trump administration tries to build a national voter file.

So far, members of Congress have rebuffed Mr. Trump's calls to nationalize elections.

"I'm not in favor of federalizing elections," Senator John Thune of South Dakota, the majority leader, told reporters on Tuesday. He said he did support stronger voter ID laws and requiring proof of citizenship at polling places, but when it comes to states having the power to run elections, that was "a constitutional issue."

The SAVE Act would require states to obtain proof of citizenship, such as a passport or a birth certificate, in person from those seeking to register to vote. It would penalize election officials for failing to seek such proof, and it would require states to proactively remove noncitizens from their voter rolls.

The House passed the bill last year, but it stalled in the Senate, where it would need the backing of at least seven Democrats to reach the 60-vote threshold to proceed to a vote.

Conservative Republicans have made a renewed push in the last few weeks to pressure the Senate to take up the bill, with far-right influencers taking to social media to criticize G.O.P. senators for not doing enough to enact the bill.

Elon Musk, a billionaire political donor, has been pushing for the bill on X, the social media platform he owns. And even as the SAVE Act has stalled, lawmakers introduced a renewed bill that would also require voters to present photo identification before voting, another long-sought goal of Republicans.

As the clamor around the bill has grown, it briefly threatened to imperil a deal to fund most of the government. Many right-wing conservatives pushed to attach a version of the SAVE Act to an unrelated spending package, and House Republican leadership needed backing from the White House to sway the holdouts to back down.

Democrats have argued that the bill is unnecessary, and that it would move to penalize officials for a problem that scarcely exists. They have also argued that its requirements were so onerous that they could discourage large swaths of

Americans from registering or voting, including women who change their name upon marriage.

“In his first term, Donald Trump pressured and threatened and coerced and incited — all in attempt to rig an election and overturn its result to cling to power,” Senator Adam B. Schiff, Democrat of California, said in a statement. “We cannot miss the signs that he is going to try again. Don’t take my word for it. Take his.”

Reid J. Epstein and Nick Corasaniti contributed reporting.

Erica L. Green is a White House correspondent for The Times, covering President Trump and his administration.

Michael Gold covers Congress for The Times, with a focus on immigration policy and congressional oversight.

Robert Jimison covers Congress for The Times, with a focus on defense issues and foreign policy.

A version of this article appears in print on , Section A, Page 14 of the New York edition with the headline: Trump Repeats Call to ‘Nationalize’ Voting as White House Walks It Back

Exhibit 2



Truth Details

9182 replies



Donald J. Trump

@realDonaldTrump

I am going to lead a movement to get rid of MAIL-IN BALLOTS, and also, while we're at it, Highly "Inaccurate," Very Expensive, and Seriously Controversial VOTING MACHINES, which cost Ten Times more than accurate and sophisticated Watermark Paper, which is faster, and leaves NO DOUBT, at the end of the evening, as to who WON, and who LOST, the Election. We are now the only Country in the World that uses Mail-In Voting. All others gave it up because of the MASSIVE VOTER FRAUD ENCOUNTERED. WE WILL BEGIN THIS EFFORT, WHICH WILL BE STRONGLY OPPOSED BY THE DEMOCRATS BECAUSE THEY CHEAT AT LEVELS NEVER SEEN BEFORE, by signing an EXECUTIVE ORDER to help bring HONESTY to the 2026 Midterm Elections. Remember, the States are merely an "agent" 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. With their HORRIBLE Radical Left policies, like Open Borders, Men Playing in Women's Sports, Transgender and "WOKE" for everyone, and so much more, Democrats are virtually Unelectable without using this completely disproven Mail-In SCAM. ELECTIONS CAN NEVER BE HONEST WITH MAIL IN BALLOTS/VOTING, and everybody, IN PARTICULAR THE DEMOCRATS, KNOWS THIS. I, AND THE REPUBLICAN PARTY, WILL FIGHT LIKE HELL TO BRING HONESTY AND INTEGRITY BACK TO OUR ELECTIONS. THE MAIL-IN BALLOT HOAX, USING VOTING MACHINES THAT ARE A COMPLETE AND TOTAL DISASTER, MUST END, NOW!!! REMEMBER, WITHOUT FAIR AND HONEST ELECTIONS, AND STRONG AND POWERFUL BORDERS, YOU DON'T HAVE EVEN A SEMBLANCE OF A COUNTRY. THANK YOU FOR YOUR ATTENTION TO THIS MATTER!!! DONALD J. TRUMP, PRESIDENT OF THE UNITED STATES OF AMERICA

19.2k ReTruths 68.4k Likes

Aug 18, 2025, 7:17 AM

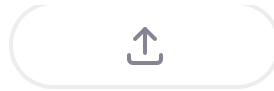
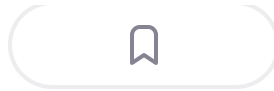
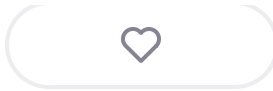
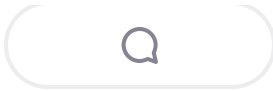


Exhibit 3

Federal Register

Vol. 91, No. 64

Friday, April 3, 2026

Presidential Documents

Title 3—

Executive Order 14399 of March 31, 2026

The President

Ensuring Citizenship Verification and Integrity in Federal Elections

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Help America Vote Act of 2002 (52 U.S.C. 20901 *et seq.*), the National Voter Registration Act of 1993 (52 U.S.C. 20501 *et seq.*), and the Federal Government's constitutional obligation to guarantee a republican form of Government to every State in the Union, U.S. Const. Art. IV, Sec. 4, it is hereby ordered:

Section 1. Purpose and Policy. The right to vote in Federal elections is reserved exclusively for citizens of the United States under the Constitution and Federal law. Federal statutes explicitly prohibit non-citizens from registering to vote or voting in Federal elections and impose criminal penalties for violations. (18 U.S.C. 241; 18 U.S.C. 611; 18 U.S.C. 1015; and 52 U.S.C. 20511). The Social Security Administration (SSA) maintains records that, in conjunction with the Department of Homeland Security's (DHS) Systematic Alien Verification for Entitlements (SAVE) program under 42 U.S.C. 1320b-7, can assist in verifying identity and Federal election voter eligibility.

The Federal Government has an unavoidable duty under Article II of the Constitution of the United States to enforce Federal law, which includes preventing violations of Federal criminal law and maintaining public confidence in election outcomes. To enhance election integrity via the United States Mail, additional measures are necessary. Secure ballot envelope identifiers provide a reliable, auditable mechanism to enforce Federal law without unduly burdening or infringing on the rights of eligible voters. Unique ballot envelope identifiers, such as bar codes, enable confirmation that only citizens receive and cast ballots, reducing the risk of fraud and protecting the integrity of Federal elections.

Sec. 2. Establishment and Transmission of State Citizenship Lists and Prioritization of Investigations and Prosecutions Related to Election Fraud. (a) To the extent feasible and consistent with applicable law, including but not limited to the Privacy Act of 1974 (5 U.S.C. 552a), the Secretary of Homeland Security, through the Director of United States Citizenship and Immigration Services and in coordination with the Commissioner of SSA, shall take appropriate action 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 List). The State Citizenship List shall be derived from Federal citizenship and naturalization records, SSA records, SAVE data, and other relevant Federal databases. The State Citizenship List shall be updated and transmitted to State election 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. The Secretary of Homeland Security shall 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 State Citizenship List transmitted thereto. An individual's identification on the State Citizenship List does not indicate that the individual has been properly registered to vote in the State. State and Federal laws and State procedures must still be followed

for an individual to be registered to vote. There may be State laws, not reflected in the State Citizenship List, that preclude voter registration, or the individual may choose not to be registered.

(b) For purposes of this order, an individual is “eligible to vote in a Federal election” if the individual is a citizen of the United States, 18 years of age or older by the date of the upcoming election, and otherwise qualified under the laws of his or her State. The Attorney General shall prioritize the investigation and, as appropriate, the prosecution of State and local officials or any others involved in the administration of Federal elections who issue Federal ballots to individuals not eligible to vote in a Federal election, including under 18 U.S.C. 2(a), 18 U.S.C. 241, 18 U.S.C. 371, 18 U.S.C. 611(a), 18 U.S.C. 1001, 18 U.S.C. 1015, 52 U.S.C. 10307, and 52 U.S.C. 20511. Similarly, the Attorney General shall prioritize the investigation and, as appropriate, the prosecution of individuals and public or private entities engaged in, or aiding and abetting, the printing, production, shipment, or distribution of ballots to individuals who are not eligible to vote in a Federal election.

Sec. 3. United States Postal Service Rulemaking on Mail-In and Absentee Ballots. (a) The unlawful use of the mail in connection with elections is prohibited by various Federal statutes, including 18 U.S.C. 1341, 18 U.S.C. 1708, 52 U.S.C. 10307, and 52 U.S.C. 20511.

(b) To ensure the faithful execution of Federal law, protect the integrity of the mail as a medium for transmitting Federal election ballots and establish uniform standards for mail-in or absentee ballot services implemented through the United States Postal Service (USPS), the Postmaster General is hereby directed to initiate a proposed rulemaking pursuant to 39 U.S.C. 401 and other applicable authority within 60 days of the date of this order. The notice of proposed rulemaking shall include, at minimum, the following:

(i) Proposed provisions specifying that all outbound ballot mail must be mailed in an envelope that:

(A) is marked as Official Election Mail, including through designated markings provided by USPS for this purpose, such as the Official Election Mail logo, as necessary and appropriate;

(B) is automation-compatible and bears a unique Intelligent Mail barcode, or successor USPS technology, that facilitates tracking and is consistent with the other requirements of this section; and

(C) has undergone a mail envelope design review by the USPS to ensure compliance with USPS mailing standards, including barcode placement.

(ii) Proposed provisions specifying that, no fewer than 90 days prior to a Federal election, any State may choose to notify the USPS if it intends to allow for mail-in or absentee ballots to be transmitted by the USPS. As part of that notification, any notifying State should further indicate whether it intends to submit to the USPS, no fewer than 60 days before the election, a list of voters eligible to vote in a Federal election in such State to whom the State intends to provide a mail-in or absentee ballot to be transmitted via the USPS.

(iii) Proposed provisions specifying that the USPS shall not transmit mail-in or absentee ballots from any individual unless those individuals have been enrolled on a State-specific list described in subsection (b)(iv) of this section with the USPS pursuant to this subsection.

(iv) Proposed provisions specifying that the USPS shall provide each State with a list of individuals (Mail-In and Absentee Participation List) who are enrolled with the USPS, pursuant to a process specified in the rulemaking directed by this subsection, for mail-in or absentee ballots provided by such State, along with unique ballot envelope identifiers, such as bar codes, for mail-in or absentee ballots provided to such individuals. The preparation and transmission of each State-specific Mail-In and Absentee Participation List shall comply with the Privacy Act and all applicable use agreements.

(v) Proposed procedures enabling each State to routinely supplement and provide suggested modifications or amendments to the State's Mail-In and Absentee Participation List in advance of any Federal election, consistent with applicable State law.

(c) The USPS shall coordinate with the USPS Office of Inspector General and the Department of Justice for investigation of suspected unlawful use of the mail involving Federal election materials.

(d) Any final rule pursuant to this section shall be issued no later than 120 days from the date of this order.

Sec. 4. Implementation. (a) The Secretary of Homeland Security, the Commissioner of SSA, and the Postmaster General shall coordinate with the Secretary of Commerce in effectuating all relevant aspects of the implementation of this order.

(b) The Attorney General shall enforce compliance with the applicable Federal statutes referenced herein and provide guidance to election officials, including any instrumentalities thereof; contractors; individuals involved in the administration of Federal elections; or public or private entities engaged in the printing, production, shipment, or distribution of ballots.

(c) The Secretary of Homeland Security shall, within 90 days of the date of this order, establish the infrastructure necessary to compile, maintain, and transmit the State Citizenship List described in section 2(a) of this order, and shall designate a point of contact within DHS to receive and process requests from individuals and State election officials regarding the relevant State Citizenship List. The Commissioner of SSA shall provide all necessary citizenship and identity data to the Secretary of Homeland Security in support of this requirement, consistent with applicable law, the Privacy Act, and all applicable use agreements.

Sec. 5. Enforcement. The Attorney General and the heads of executive departments and agencies (agencies) with relevant authority shall take all lawful steps to deter and address noncompliance with Federal law, including withholding Federal funds from noncompliant States and localities where such withholding is authorized by law. Evidence of violations of existing Federal laws by State or local election officials; States or localities, including any instrumentalities thereof; contractors; individuals involved in the administration of Federal elections; or public or private entities engaged in the printing, production, shipment, or distribution of ballots may be referred to the Department of Justice for consideration of investigation or charges under 18 U.S.C. 2(a), 18 U.S.C. 241, 18 U.S.C. 371, 18 U.S.C. 611(a), 18 U.S.C. 1001, 18 U.S.C. 1015, 52 U.S.C. 10307, and 52 U.S.C. 20511. States and localities should preserve, for a 5-year period, all records and materials—excluding ballots cast—evidencing voter participation in any Federal election (e.g., ballot envelopes, regardless of carrier).

Sec. 6. Severability. If any provision of this order, or the application of any provision to any agency, person, or circumstance, is held to be invalid, the remainder of this order and the application of its provisions to any other agencies, persons, or circumstances shall not be affected thereby.

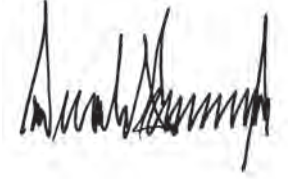
Sec. 7. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

A handwritten signature in black ink, appearing to be a stylized name, possibly "Donald Trump", written in a cursive script.

THE WHITE HOUSE,
March 31, 2026.

Exhibit 4

Presidential Documents

Executive Order 14248 of March 25, 2025

Preserving and Protecting the Integrity of American Elections

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose and Policy. Despite pioneering self-government, the United States now fails to enforce basic and necessary election protections employed by modern, developed nations, as well as those still developing. India and Brazil, for example, are tying voter identification to a biometric database, while the United States largely relies on self-attestation for citizenship. In tabulating votes, Germany and Canada require use of paper ballots, counted in public by local officials, which substantially reduces the number of disputes as compared to the American patchwork of voting methods that can lead to basic chain-of-custody problems. Further, while countries like Denmark and Sweden sensibly limit mail-in voting to those unable to vote in person and do not count late-arriving votes regardless of the date of postmark, many American elections now feature mass voting by mail, with many officials accepting ballots without postmarks or those received well after Election Day.

Free, fair, and honest elections unmarred by fraud, errors, or suspicion are fundamental to maintaining our constitutional Republic. The right of American citizens to have their votes properly counted and tabulated, without illegal dilution, is vital to determining the rightful winner of an election.

Under the Constitution, State governments must safeguard American elections in compliance with Federal laws that protect Americans' voting rights and guard against dilution by illegal voting, discrimination, fraud, and other forms of malfeasance and error. Yet the United States has not adequately enforced Federal election requirements that, for example, prohibit States from counting ballots received after Election Day or prohibit non-citizens from registering to vote.

Federal law establishes a uniform Election Day across the Nation for Federal elections, 2 U.S.C. 7 and 3 U.S.C. 1. It is the policy of my Administration to enforce those statutes and require that votes be cast and received by the election date established in law. As the United States Court of Appeals for the Fifth Circuit recently held in *Republican National Committee v. Wetzel* (2024), those statutes set "the day by which ballots must be both cast by voters and received by state officials." Yet numerous States fail to comply with those laws by counting ballots received after Election Day. This is like allowing persons who arrive 3 days after Election Day, perhaps after a winner has been declared, to vote in person at a former voting precinct, which would be absurd. Several Federal laws, including 18 U.S.C. 1015 and 611, prohibit foreign nationals from registering to vote or voting in Federal elections. Yet States fail adequately to vet voters' citizenship, and, in recent years, the Department of Justice has failed to prioritize and devote sufficient resources for enforcement of these provisions. Even worse, the prior administration actively prevented States from removing aliens from their voter lists.

Additionally, Federal laws, such as the National Voter Registration Act (Pub. L. 103–31) and the Help America Vote Act (Pub. L. 107–252), require States to maintain an accurate and current Statewide list of every legally registered voter in the State. And the Department of Homeland Security is required to share database information with States upon request so they

can fulfill this duty. See 8 U.S.C. 1373(c). Maintaining accurate voter registration lists is a fundamental requirement in protecting voters from having their ballots voided or diluted by fraudulent votes.

Federal law, 52 U.S.C. 30121, prohibits foreign nationals from participating in Federal, State, or local elections by making any contributions or expenditures. But foreign nationals and non-governmental organizations have taken advantage of loopholes in the law's interpretation, spending millions of dollars through conduit contributions and ballot-initiative-related expenditures. This type of foreign interference in our election process undermines the franchise and the right of American citizens to govern their Republic.

Above all, elections must be honest and worthy of the public trust. That requires voting methods that produce a voter-verifiable paper record allowing voters to efficiently check their votes to protect against fraud or mistake. Election-integrity standards must be modified accordingly.

It is the policy of my Administration to enforce Federal law and to protect the integrity of our election process.

Sec. 2. *Enforcing the Citizenship Requirement for Federal Elections.* To enforce the Federal prohibition on foreign nationals voting in Federal elections:

(a)(i) Within 30 days of the date of this order, the Election Assistance Commission shall take appropriate action to require, in its national mail voter registration form issued under 52 U.S.C. 20508:

(A) documentary proof of United States citizenship, consistent with 52 U.S.C. 20508(b)(3); and

(B) a State or local official to record on the form the type of document that the applicant presented as documentary proof of United States citizenship, including the date of the document's issuance, the date of the document's expiration (if any), the office that issued the document, and any unique identification number associated with the document as required by the criteria in 52 U.S.C. 21083(a)(5)(A), while taking appropriate measures to ensure information security.

(ii) For purposes of subsection (a) of this section, "documentary proof of United States citizenship" shall include a copy of:

(A) a United States passport;

(B) an identification document compliant with the requirements of the REAL ID Act of 2005 (Pub. L. 109–13, Div. B) that indicates the applicant is a citizen of the United States;

(C) an official military identification card that indicates the applicant is a citizen of the United States; or

(D) a valid Federal or State government-issued photo identification if such identification indicates that the applicant is a United States citizen or if such identification is otherwise accompanied by proof of United States citizenship.

(b) To identify unqualified voters registered in the States:

(i) the Secretary of Homeland Security shall, consistent with applicable law, ensure that State and local officials have, without the requirement of the payment of a fee, access to appropriate systems for verifying the citizenship or immigration status of individuals registering to vote or who are already registered;

(ii) the Secretary of State shall take all lawful and appropriate action to make available information from relevant databases to State and local election officials engaged in verifying the citizenship of individuals registering to vote or who are already registered; and

(iii) the Department of Homeland Security, in coordination with the DOGE Administrator, shall review each State's publicly available voter registration list and available records concerning voter list maintenance activities as

required by 52 U.S.C. 20507, alongside Federal immigration databases and State records requested, including through subpoena where necessary and authorized by law, for consistency with Federal requirements.

(c) Within 90 days of the date of this order, the Secretary of Homeland Security shall, consistent with applicable law, provide to the Attorney General complete information on all foreign nationals who have indicated on any immigration form that they have registered or voted in a Federal, State, or local election, and shall also take all appropriate action to submit to relevant State or local election officials such information.

(d) The head of each Federal voter registration executive department or agency (agency) under the National Voter Registration Act, 52 U.S.C. 20506(a), shall assess citizenship prior to providing a Federal voter registration form to enrollees of public assistance programs.

(e) The Attorney General shall prioritize enforcement of 18 U.S.C. 611 and 1015(f) and similar laws that restrict non-citizens from registering to vote or voting, including through use of:

(i) databases or information maintained by the Department of Homeland Security;

(ii) State-issued identification records and driver license databases; and

(iii) similar records relating to citizenship.

(f) The Attorney General shall, consistent with applicable laws, coordinate with State attorneys general to assist with State-level review and prosecution of aliens unlawfully registered to vote or casting votes.

Sec. 3. *Providing Other Assistance to States Verifying Eligibility.* To assist States in determining whether individuals are eligible to register and vote:

(a) The Commissioner of Social Security shall take all appropriate action to make available the Social Security Number Verification Service, the Death Master File, and any other Federal databases containing relevant information to all State and local election officials engaged in verifying the eligibility of individuals registering to vote or who are already registered. In determining and taking such action, the Commissioner of Social Security shall ensure compliance with applicable privacy and data security laws and regulations.

(b) The Attorney General shall ensure compliance with the requirements of 52 U.S.C. 20507(g).

(c) The Attorney General shall take appropriate action with respect to States that fail to comply with the list maintenance requirements of the National Voter Registration Act and the Help America Vote Act contained in 52 U.S.C. 20507 and 52 U.S.C. 21083.

(d) The Secretary of Defense shall update the Federal Post Card Application, pursuant to the Uniformed and Overseas Citizens Absentee Voting Act, 52 U.S.C. 20301, to require:

(i) documentary proof of United States citizenship, as defined by section 2(a)(ii) of this order; and

(ii) proof of eligibility to vote in elections in the State in which the voter is attempting to vote.

Sec. 4. *Improving the Election Assistance Commission.* (a) The Election Assistance Commission shall, pursuant to 52 U.S.C. 21003(b)(3) and 21142(c) and consistent with applicable law, take all appropriate action to cease providing Federal funds to States that do not comply with the Federal laws set forth in 52 U.S.C. 21145, including the requirement in 52 U.S.C. 20505(a)(1) that States accept and use the national mail voter registration form issued pursuant to 52 U.S.C. 20508(a)(1), including any requirement for documentary proof of United States citizenship adopted pursuant to section 2(a)(ii) of this order.

(b)(i) The Election Assistance Commission shall initiate appropriate action to amend the Voluntary Voting System Guidelines 2.0 and issue other appropriate guidance establishing standards for voting systems to protect election

integrity. The amended guidelines and other guidance shall provide that voting systems should not use a ballot in which a vote is contained within a barcode or quick-response code in the vote counting process except where necessary to accommodate individuals with disabilities, and should provide a voter-verifiable paper record to prevent fraud or mistake.

(ii) Within 180 days of the date of this order, the Election Assistance Commission shall take appropriate action to review and, if appropriate, re-certify voting systems under the new standards established under subsection (b)(i) of this section, and to rescind all previous certifications of voting equipment based on prior standards.

(c) Following an audit of Help America Vote Act fund expenditures conducted pursuant to 52 U.S.C. 21142, the Election Assistance Commission shall report any discrepancies or issues with an audited State's certifications of compliance with Federal law to the Department of Justice for appropriate enforcement action.

(d) The Secretary of Homeland Security and the Administrator of the Federal Emergency Management Agency, consistent with applicable law, shall in considering the provision of funding for State or local election offices or administrators through the Homeland Security Grant Programs, 6 U.S.C. 603 *et seq.*, heavily prioritize compliance with the Voluntary Voting System Guidelines 2.0 developed by the Election Assistance Commission and completion of testing through the Voting System Test Labs accreditation process.

Sec. 5. Prosecuting Election Crimes. To protect the franchise of American citizens and their right to participate in fair and honest elections:

(a) The Attorney General shall take all appropriate action to enter into information-sharing agreements, to the maximum extent possible, with the chief State election official or multi-member agency of each State. These agreements shall aim to provide the Department of Justice with detailed information on all suspected violations of State and Federal election laws discovered by State officials, including information on individuals who:

- (i) registered or voted despite being ineligible or who registered multiple times;
- (ii) committed election fraud;
- (iii) provided false information on voter registration or other election forms;
- (iv) intimidated or threatened voters or election officials; or
- (v) otherwise engaged in unlawful conduct to interfere in the election process.

(b) To the extent that any States are unwilling to enter into such an information sharing agreement or refuse to cooperate in investigations and prosecutions of election crimes, the Attorney General shall:

- (i) prioritize enforcement of Federal election integrity laws in such States to ensure election integrity given the State's demonstrated unwillingness to enter into an information-sharing agreement or to cooperate in investigations and prosecutions; and
- (ii) review for potential withholding of grants and other funds that the Department awards and distributes, in the Department's discretion, to State and local governments for law enforcement and other purposes, as consistent with applicable law.

(c) The Attorney General shall take all appropriate action to align the Department of Justice's litigation positions with the purpose and policy of this order.

Sec. 6. Improving Security of Voting Systems. To improve the security of all voting equipment and systems used to cast ballots, tabulate votes, and report results:

(a) The Attorney General and the Secretary of Homeland Security shall take all appropriate actions to the extent permitted by 42 U.S.C. 5195c

and all other applicable law, so long as the Department of Homeland Security maintains the designation of election infrastructure as critical infrastructure, as defined by 42 U.S.C. 5195c(e), to prevent all non-citizens from being involved in the administration of any Federal election, including by accessing election equipment, ballots, or any other relevant materials used in the conduct of any Federal election.

(b) The Secretary of Homeland Security shall, in coordination with the Election Assistance Commission and to the maximum extent possible, review and report on the security of all electronic systems used in the voter registration and voting process. The Secretary of Homeland Security, as the head of the designated Sector Risk Management Agency under 6 U.S.C. 652a, in coordination with the Election Assistance Commission, shall assess the security of all such systems to the extent they are connected to, or integrated into, the Internet and report on the risk of such systems being compromised through malicious software and unauthorized intrusions into the system.

Sec. 7. Compliance with Federal Law Setting the National Election Day. To achieve full compliance with the Federal laws that set the uniform day for appointing Presidential electors and electing members of Congress:

(a) The Attorney General shall take all necessary action to enforce 2 U.S.C. 7 and 3 U.S.C. 1 against States that violate these provisions by including absentee or mail-in ballots received after Election Day in the final tabulation of votes for the appointment of Presidential electors and the election of members of the United States Senate and House of Representatives.

(b) Consistent with 52 U.S.C. 21001(b) and other applicable law, the Election Assistance Commission shall condition any available funding to a State on that State's compliance with the requirement in 52 U.S.C. 21081(a)(6) that each State adopt uniform and nondiscriminatory standards within that State that define what constitutes a vote and what will be counted as a vote, including that, as prescribed in 2 U.S.C. 7 and 3 U.S.C. 1, there be a uniform and nondiscriminatory ballot receipt deadline of Election Day for all methods of voting, excluding ballots cast in accordance with 52 U.S.C. 20301 *et seq.*, after which no additional votes may be cast.

Sec. 8. Preventing Foreign Interference and Unlawful Use of Federal Funds. The Attorney General, in consultation with the Secretary of the Treasury, shall prioritize enforcement of 52 U.S.C. 30121 and other appropriate laws to prevent foreign nationals from contributing or donating in United States elections. The Attorney General shall likewise prioritize enforcement of 31 U.S.C. 1352, which prohibits lobbying by organizations or entities that have received any Federal funds.

Sec. 9. Federal Actions to Address Executive Order 14019. The heads of all agencies, and the Election Assistance Commission, shall cease all agency actions implementing Executive Order 14019 of March 7, 2021 (Promoting Access to Voting), which was revoked by Executive Order 14148 of on January 20, 2025 (Initial Rescissions of Harmful Executive Orders and Actions), and, within 90 days of the date of this order, submit to the President, through the Assistant to the President for Domestic Policy, a report describing compliance with this order.

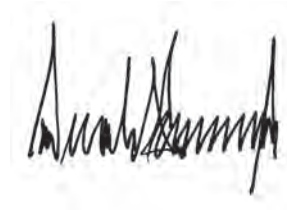
Sec. 10. Severability. If any provision of this order, or the application of any provision to any agency, person, or circumstance, is held to be invalid, the remainder of this order and the application of its provisions to any other agencies, persons, or circumstances shall not be affected thereby.

Sec. 11. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

- (i) the authority granted by law to an executive department or agency, or the head thereof; or
- (ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

A handwritten signature in black ink, appearing to be a stylized name, possibly "Donald Trump", written in a cursive script.

THE WHITE HOUSE,
March 25, 2025.

Exhibit 5

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND

<p>* * * * *</p> <p>UNITED STATES OF AMERICA,</p> <p style="padding-left: 40px;">Plaintiff,</p> <p style="padding-left: 80px;">vs.</p> <p>GREGG M. AMORE, in his official capacity as Secretary of State for the State of Rhode Island,</p> <p style="padding-left: 40px;">Defendant.</p> <p>* * * * *</p>	<p>*25-CV-639-MSM</p> <p>*</p> <p>*</p> <p>*</p> <p>*</p> <p>*MARCH 26, 2026</p> <p>*</p> <p>*</p> <p>*</p> <p>*</p> <p>*Courtroom 2</p> <p>*PROVIDENCE, RI</p> <p>*</p>
--	--

BEFORE THE HONORABLE MARY S. McELROY
DISTRICT JUDGE

(Motion to Compel)
(Motions to Dismiss)

APPEARANCES:

<p>FOR THE PLAINTIFF:</p> <p>FOR THE DEFENDANT: Gregg Amore</p>	<p>ERIC NEFF DOJ-Crt Civil Rights Division 150 M St. NE, Ste 8-1807 Washington, DC 20002</p> <p>JAMES J. ARGUIN RI Department of Attorney General 150 South Main Street Providence, RI 02903</p>
--	---

1 FOR INTERVENOR DEFENDANTS:

2 Common Cause ARI J. SAVITZKY
3 Catherine Saunders American Civil Liberties Union
4 Stuart Waldman Foundation
5 Julia Sanches 125 Broad Street
New York, NY 10004

5 FOR INTERVENOR DEFENDANTS:

6 SEIU District 1199NE ROBERT GOLAN-VILELLA, ESQ.
7 Rhode Island Alliance for Elias Law Group LLP
8 Retired Americans 250 Massachusetts Ave NW
Carolyn Betensky Ste 400
Michael Zack Mezera Washington, DC 20001

9

10 Court Reporter: Denise P. Veitch, RPR
11 One Exchange Terrace
12 Providence, RI 02903

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 non-public lists; correct?

2 THE COURT: Right.

3 MR. NEFF: Okay. The United States is taking
4 extra concern to make sure that we're complying with
5 the Privacy Act in every conceivable way, and there are
6 still a couple steps we have to go through before the
7 United States is comfortable proceeding and comfortable
8 representing to this Court that we're in full
9 compliance with the Privacy Act.

10 THE COURT: What steps have you taken and what
11 steps need to be taken with those states that have
12 complied? Because to me, the states that have complied
13 are traditionally more conservative states. Texas just
14 gave you their list, let's say. Why not go through
15 Texas's list to make sure that only eligible voters are
16 on their list?

17 MR. NEFF: I can only go into the United States
18 delivery of process so much, you Honor, but what I can
19 say is that the United States is evaluating, for one,
20 an opinion out of the D.C. Circuit that analyzed DHS's
21 SORN, and also the United States is -- we are certainly
22 going to be proceeding with running this, our intention
23 is to run this against DHS's SAVE database.

24 THE COURT: Which database?

25 MR. NEFF: The SAVE database that runs, that

1 essentially is a, it's called like a fetching system
2 that seeks information from other databases to
3 cross-check whether the data set on a roll is either a
4 deceased person or a noncitizen.

5 THE COURT: And what's the accuracy rate of data
6 that you've run against that system?

7 MR. NEFF: The accuracy rate we've been told --

8 THE COURT: By whom?

9 MR. NEFF: -- by DHS, and it's particularly the
10 SAVE personnel that run the system is that it is in
11 effect 100 percent accurate.

12 THE COURT: That's not the reporting; right? I
13 mean isn't the reporting that people have been run
14 through that SAVE Act and not for voting but for other
15 things have been kicked out as noncitizens when they
16 were, in fact, citizens?

17 MR. NEFF: There's an important note that the
18 SAVE database has been around, the SAVE Act,
19 essentially states have been able to submit their
20 information to SAVE for about 30 years. But SAVE has
21 also changed drastically in the last few months. It's
22 been I would call upgraded and the process they go
23 through, we can go into that if your Honor wants to,
24 but essentially when any flagged voter comes back, it's
25 then run through a very comprehensive confirmation

1 process to make sure that the, quote, like problematic
2 registration is, in fact, not just --

3 THE COURT: What's the process?

4 MR. NEFF: DHS has about 200-odd employees who
5 are trained for a minimum of six months each and know
6 various databases that are accessible to the federal
7 government through use and shared agreements to be able
8 to essentially access important naturalization files
9 and other data that can establish whether the person is
10 a citizen, because there are holes in the process.

11 THE COURT: What are the holes?

12 MR. NEFF: The holes, the most common hole would
13 be when someone is -- someone who came to the United
14 States is a parent and has children who are U.S.
15 citizens and then naturalized; like the most common
16 hole of that is that it's actually rather expensive to
17 go through the full, quote, documentation process. A
18 common, cheaper shortcut that people will just do is
19 just go get a passport.

20 THE COURT: By "people," do you mean the
21 children or the parent?

22 MR. NEFF: The parents, your Honor.

23 THE COURT: Because the children are derivative
24 citizens under that scenario, so even if the children
25 are born outside of the United States; correct?

1 MR. NEFF: Correct. And I'm talking about the
2 parent in this scenario as the most common problematic
3 scenario; that the child is not a problem. That would
4 not come up as any issue. It's the parent that
5 potentially would and --

6 THE COURT: If they're naturalized they can't
7 vote?

8 MR. NEFF: Explaining to your Honor when an
9 immigrant is naturalized, sometimes that's not
10 immediately available in naturalization documentation
11 databases. So what these 200 people are doing is
12 they're going to other ways to verify that that person
13 a citizen. One common way is going to the Department
14 of State and confirming that they have a passport.

15 THE COURT: Gotcha. So what you're saying, what
16 you're asserting here is the federal government's role
17 in that process. That's not what the Framers
18 envisioned, is it? The Framers gave in the Elections
19 Clause the responsibility for maintaining elections to
20 the individual states, with some congressional
21 oversight or some congressional barriers or, what do
22 you call them, check points.

23 But it's not a federal government role to
24 maintain -- to run elections. It never has been. I
25 mean we're supposed to look at what the original intent

1 the snapshot right in time that is used for an actual
2 election.

3 THE COURT: But isn't your role more effectively
4 -- and I'm not going to pretend to tell the Department
5 of Justice how to do their job. But why would you not
6 be looking at the processes that states are using, as
7 opposed to the list? The list gives you nothing except
8 a snapshot in time. The process tells you whether or
9 not they're complying with HAVA and the National Voting
10 Rights Act.

11 MR. NEFF: We look at both, your Honor, and --

12 THE COURT: Why does the list help?

13 MR. NEFF: Because the United States has the
14 capability to run these lists against other databases
15 to be able to tell if there are bad registrations on
16 their rolls.

17 THE COURT: So if I -- I'm registered to vote in
18 Rhode Island. If I move to Oregon and register, and
19 you get the list where I'm still in Rhode Island, then
20 that somehow says Rhode Island's list is inaccurate,
21 even if I never voted here after I moved.

22 MR. NEFF: No, your Honor. It just leads to a
23 scenario where we can check with Rhode Island, do our
24 constitutional and statutory duty to verify with Rhode
25 Island they have removed you from the rolls.

1 don't have to tell you why, essentially.

2 MR. NEFF: Far from acknowledging the new era
3 we're in, we're embracing it. This is just a first
4 step to sifting down to where there are problematic
5 registrations. I think it would fair for someone to
6 state that in today's day and age it's extremely hard
7 to comply with all the provisions at the HAVA at the
8 scale the Secretaries of the State are being asked to
9 do right now. We can work as a partner with them.
10 This is only a first step to seeing where some of the
11 problems may be; and so because of such a large number
12 as Rhode Island themselves has said, we need to be able
13 to do our initial check so that we can start whittling
14 down where maybe some of the problems are. We're not
15 saying there are problems. That's not what we're
16 talking about at this phase. We're just talking about
17 doing the initial screening that is necessary, given
18 the scale of a voter registration list.

19 THE COURT: But the Department of Justice kind
20 of came in hot and asked for all the information. They
21 didn't say, hey, let's partner, how can we help you,
22 what are you doing? They came in and said give us all
23 your information because we need to verify that you're
24 doing what you're supposed to be doing, so offering a
25 partnership now seems a little hollow.

Exhibit 6

UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA,)	
Plaintiff,)	No: 3:26-cv-00021-KAD
)	
v.)	March 19, 2026
STEPHANIE THOMAS, <i>in her Official</i>)	
<i>Capacity as Secretary of State for</i>)	
<i>the State of Connecticut, ET AL.,</i>)	
Defendants.)	10:08 a.m.

Brien McMahon Federal Building
915 Lafayette Boulevard
Bridgeport, CT 06604

HEARING
Re: Order to Show Cause

B E F O R E:
THE HONORABLE KARI A. DOOLEY, U.S.D.J.

Courtroom Deputy:
Abby Bociek

Official Court Reporter:
Tracy L. Gow, RPR

Chambers: 203.579.5522

1 MR. TUCKER: If the United States becomes aware that
2 there are non-citizens on the list, and in some cases States
3 have told us they have non-citizens on the list, at that
4 point --

5 THE COURT: Has Connecticut told you it has
6 non-citizens on the list?

7 MR. TUCKER: No, not to my knowledge, Your Honor.

8 THE COURT: Okay.

9 MR. TUCKER: But, again, also consistent with the
10 fact that we are the Civil Rights Division, those are issues
11 that, typically, when we become aware of them, we reach out
12 to the State and indicate, or if they've told us that we have
13 non-citizens, you know, we engage in a dialogue with the
14 State to determine what actions, if any, they're going to
15 take.

16 In the event that they're not going to take any
17 actions, those are typically matters that are taken up, if
18 it's appropriate, that the Criminal Division would look at it
19 or the local U.S. Attorney's Office would do it. But, again,
20 it's not something that the Civil Rights Division would do.

21 THE COURT: So when -- if you get these voter rolls,
22 you're going to analyze them to see if there are duplicates;
23 yes?

24 MR. TUCKER: Yes, Your Honor.

25 THE COURT: And you're going to run them through the

1 Social Security's list of deceased people to see if there are
2 any deceased people on it?

3 MR. TUCKER: Yes, Your Honor.

4 THE COURT: But you're not going to take any
5 affirmative steps to try to determine whether there are
6 non-citizens on it?

7 MR. TUCKER: With non-citizens, the United States --
8 in the event the decision is made to do that, the United
9 States would have to enter into a memorandum of understanding
10 with DHS. And the way it's been explained to me, DHS never
11 comes into possession of it. What it is, is it's run
12 directly against the SAVE database.

13 You have a user-specific password that you enter so
14 that the data is never retained. DHS can't do anything with
15 it, because it's being run through their database, but they
16 never have -- they never have any specific access to it
17 because, again, they never actually see anything that's being
18 run through the SAVE database.

19 And, again, that would require a memorandum of
20 understanding with the Department of Homeland Security. And,
21 of course, it would be subject to whatever limitations, if
22 any, that the Court puts in an appropriate tailored order,
23 getting to your third question that we won't get to.

24 THE COURT: Okay. Thank you.

25 MR. TUCKER: Thank you, Your Honor.

1 provided voter rolls, has that data been provided to any
2 other agencies?

3 MR. TUCKER: For those states, I don't believe so,
4 no. Again, part of it is that we're also in the process of
5 getting memorandum of understanding with -- for example,
6 Social Security Administration. I don't know what the status
7 of that is. I don't believe it's happened yet.

8 As counsel has certainly suggested, we're dealing
9 with a very large number of records. So just even the
10 processing of the records coming in and making sure that
11 they're securely stored has been the -- first and foremost,
12 the task that we've been undertaking.

13 THE COURT: And do you know if they've been run
14 through the SAVE database with DHS?

15 MR. TUCKER: No, none of the private -- private
16 information that's been produced to us has been run through a
17 SAVE database.

18 My understanding is that there has been public
19 information that -- again, this is public information you can
20 download from many states -- I don't know if Connecticut
21 makes its database readily available, but my understanding is
22 that publicly available information that anyone can do, I
23 could get on my phone right now and start downloading it,
24 that that information has been run through the SAVE database.
25 But, again, it doesn't include any personally identifiable

Exhibit 7

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

Plaintiff,

v.

WILLIAM FRANCIS GALVIN, in his
Official Capacity as Secretary of State for
the Commonwealth of Massachusetts,

Defendant(s).

Case Number: 1:25-cv-13816-LTS

DECLARATION OF ERIC NEFF IN SUPPORT OF THE UNITED STATES' MOTION TO COMPEL (DOC. 6) AND IN OPPOSITION TO MOTIONS TO DISMISS BY DEF. GALVIN (DOC. 56), INTERVENOR-DEF. COMMON CAUSE, JANE DOE INC., JUAN PABLO JARAMILLO (DOC. 49), AND MASS ALLIANCE FOR RETIRED AMERICAMNS, NEW ENGLAND STATE ARE CONFERENCE OF THE NAACP (DOC. 52)

DECLARATION

I, Eric Neff, declare, pursuant to 28 U.S.C. § 1746, that:

1. I am currently Acting Chief to the Voting Section within the Civil Rights Division of the United States Department of Justice. I am fully and personally familiar with the facts stated herein. I make this declaration in support of the United States' Motion to Compel the production of election records pursuant to the Civil Rights Act codified at 52 U.S.C. §§ 20701, *et seq.* (Doc. 6) and in opposition to Defendants' Motions to Dismiss (Docs. 56, 49, and 52), and to supplement the Declaration of Eric Neff dated December 12, 2025 (Doc. 6-1).
2. As stated in the correspondence dated August 14, 2025 attached as Exhibit 3 to the Mem. in Supp. Motion to Compel (Doc. 7-3) the United States has requested the federal

election records that are the subject of this litigation for the limited purpose of evaluating Massachusetts' compliance with the list maintenance provisions of the Help America Vote Act ("HAVA") and the National Voter Registration Act ("NVRA"), and, if appropriate, to bring an enforcement action.

3. HAVA requires that "an application for voter registration for an election for Federal office may not be accepted or processed by a State unless the application includes" the applicant's driver's license number or if that is unavailable, the last four digits of the Social Security number. 52 U.S.C. § 21083(a)(5)(A)(i). That information is necessary to identify duplicate registration records, registrants who have moved, registrants who have died, and those who are not eligible to vote in federal elections.
4. To ascertain whether a jurisdiction engages in practices that violate federal law (whether HAVA, the NVRA, the Voting Rights Act or any other one), the Attorney General needs to examine both applications to register to vote *and* the final voting rolls, including the electronic statewide voter registration list ("SVRL"), so as to assure herself that the applications are being properly processed and that reasonable and nondiscriminatory list maintenance efforts have been practiced.
5. Contrary to what Defendant-Intervenors contend through third-party hearsay, the records the United States is seeking to compel under the CRA are not intended "to create a nationwide voter list, an unprecedented scheme not authorized by any source of law." Mem. in Supp. of New England State Area Conference of the NAACP and the Massachusetts Alliance for Retired Americans' Mot. to Dismiss, Doc. 54 at 4. Rather, the records sought from Massachusetts are necessary to perform an individualized assessment of the State's efforts to comply with HAVA and the NVRA.

6. When the Civil Rights Division performs this individualized assessment, the State's SVRL is compartmentalized and maintained by the Civil Rights Division separately from the SVRL of any other State. The maintenance, use, and destruction of those records is in full compliance with the requirements in the CRA, Privacy Act, and all other federal laws governing the records.
7. The United States previously has pursued successful matters, including in litigation, to obtain statewide voter registration lists under Title III of the Civil Rights Act ("CRA").
8. For example, in two of those CRA matters against Georgia and Texas, the United States obtained the SVRLs, including drivers' license numbers and last four digits of the registrant's social security number, to evaluate compliance with the NVRA, including that Act's list maintenance requirements.
9. A true and accurate copy of the Complaint filed in *United States v. Georgia*, Case No. 1:06-cv-02442-CC (N.D. Ga. filed Oct. 12, 2006), is attached as Exhibit 1.
10. On October 27, 2006, the Court entered a Consent Decree in *Georgia* requiring the state to produce its SVRL to the United States. A true and accurate copy of the *Georgia* Consent Decree is attached as Exhibit 2.
11. The Texas matter was resolved by a Memorandum of Understanding ("MOU") dated May 13, 2008, which required Texas to produce its SVRL to the United States. A true and accurate copy of the Texas MOU is attached as Exhibit 3.
12. Recent enforcement efforts by the Attorney General demonstrate the need for federal scrutiny, as Congress contemplated in authorizing the Attorney General to bring enforcement actions under HAVA and the NVRA.

13. In 2025, North Carolina election officials admitted that the state “maintained and used a HAVA List that includes records that do not comply with the requirements for Federal elections under Section 303(a)(5).” *United States v. N. Carolina Bd. of Elections*, Case No. 5:25-cv-00283-M-RJ Consent J. & Order at 4 (E.D.N.C. Sept. 8, 2025). Specifically, the State’s HAVA List included over one hundred thousand active voter records that were missing one of the identification numbers required by HAVA: the registrant’s driver’s license number, the last four numbers of the registrant’s social security number, or a unique identifying number if the registrant had neither a driver’s license nor a social security number. A true and accurate copy of the *North Carolina* Consent Judgment and Order is attached as Exhibit 4.
14. As a result of the Attorney General’s enforcement action, North Carolina has reduced the number of voter records missing an identification number under HAVA from 103,329 to 70,709. *See N. Carolina Bd. of Elections*, Defs.’ 2d Status R. at 2 (E.D.N.C. Jan. 30, 2026). A true and accurate copy of the Second Status Report from the *North Carolina* litigation is attached as Exhibit 5.
15. As stated in my first Declaration, the United States reached out to Massachusetts to address any reasonable privacy concerns without impeding the Attorney General’s authority to enforce federal law.
16. To that end, the United States has offered various states an MOU memorializing these requirements. As of February 27, 2026, eighteen states either have provided their SVRL or indicated they will be doing so including: thirteen states that have provided their SVRLs without any MOU; two states that have agreed to provide their SVRL under the terms of the MOU; and three states that are likely to provide the SVRLs soon.

17. An Initial Privacy Assessment (IPA) Determination was issued on October 12, 2012, showing that no Privacy Impact Assessment is required for the Justice Consolidated Office Network (JCON) system where personal identifying information associated with the United States' CRA demand is stored.
18. A true and accurate copy of cited excerpts from the report by the National Commission on Federal Election Reform (the Ford-Carter Commission), entitled "To Assure Pride and Confidence in the Electoral Process (Aug. 2001)," is attached as Exhibit 6.
19. A true and accurate copy of the Notice of Appeal filed in *United States v. Benson*, Case No. 1:25-cv-01148-HYJ-PJG, 2026 WL 362789 (W.D. Mich. Feb. 10, 2026), is attached as Exhibit 7.
20. A true and accurate copy of the Notice of Appeal filed in *United States v. Oregon*, Case No. 6:25-cv-01666-MTK, 2026 WL 318402 (D. Or. Feb. 5, 2026), is attached as Exhibit 8.
21. A true and accurate copy of the Notice of Appeal filed in *United States v. Weber*, Case No. 2:25-cv-09149-DOC-ADS, 2026 WL 118807 (C.D. Cal. Jan. 15, 2026), is attached as Exhibit 9.

I declare under the penalty of perjury that the above statements are true and correct. Executed on February 27, 2026.

Dated: February 27, 2026, at Washington, D.C.

/s/Eric Neff

Eric Neff

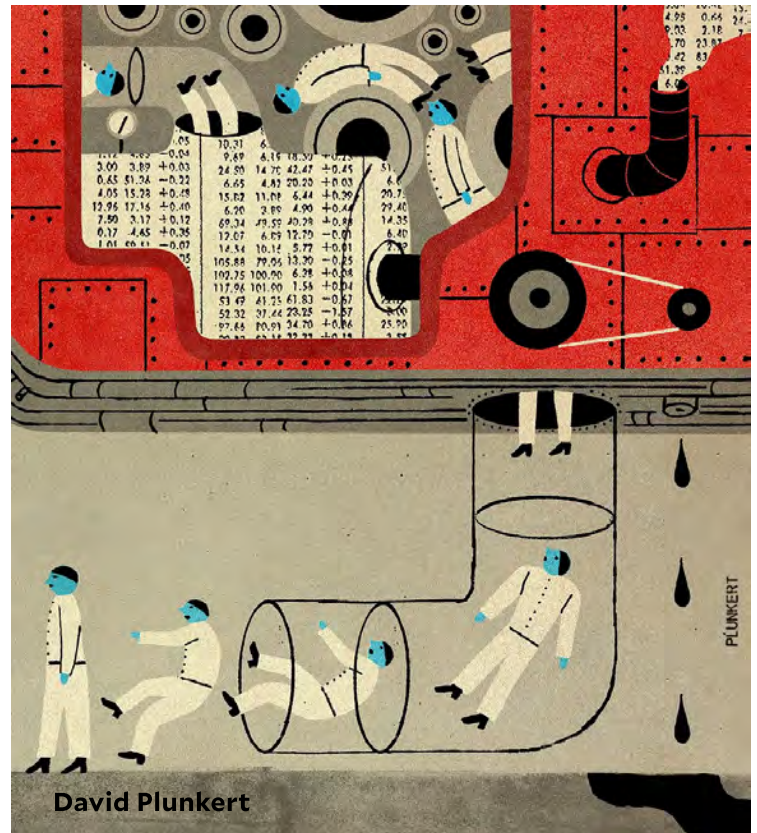
Exhibit 8

THE BIG FEATURE

Your Private Data Is Building Trump's Voter Purge Machine

The Justice Department ordinarily would prevent attacks on voting rights. Now it's carrying them out.

ABBY VESOULIS AND ARI
BERMAN DECEMBER 5, 2025



Get your news from a source that's not owned and controlled by oligarchs. Sign up for the free Mother Jones Daily.

It was National Voter Registration Day, and Maine Secretary of State Shenna Bellows was on her way to a small liberal arts college for a voter registration event. That's when she learned the US Department of Justice was suing her over how she manages Maine's voter registrant list.

While the DOJ appearing as the official plaintiff was new, what the federal government sought through the lawsuit—access to Maine's complete, unredacted voter roll file—was not.

Bellows, a spunky, no-nonsense 50-year-old who grew up in a log cabin without running water, already had received a litany of demand letters, public records requests, and lawsuits throughout her five years serving as the top election integrity official in Maine. Citing the National Voter Registration Act, most of the requests for the state's voter data had the ostensible aim of ensuring Maine was adequately removing the names of individuals who should not be on the voter roll. But this lawsuit was the first of its kind from the government itself.

The September legal complaint was an escalation of a yearslong coordinated effort by conservatives to obtain voter roll data from numerous states, compare it to incomplete datasets they'd found on the commercial market, then attest that mismatches between the two are clear evidence of people illegally voting. The apparent goal: buttressing decadeslong, though still unproven, claims of rampant voter fraud and removing allegedly ineligible voters from the rolls, with potentially dire consequences for future elections.

In the past, these sorts of legal gambits came from right-wing groups like the America First Policy Institute, a Trump-aligned think tank co-founded by Brooke Rollins, now the secretary of agriculture; the Dhillon Law Group, whose founder, Harmeet Dhillon, is now the assistant attorney general for civil rights at the DOJ; and the Public Interest

Legal Foundation (PILF), a conservative legal group whose former counsel, Maureen Riordan, now leads the DOJ's voting section. Riordan and Dhillon remain in the same line of business, citing familiar statutes in their barrage of new lawsuits against state election officials like Bellows; the key difference now is that they are promoting their routinely debunked theories from *within* the US government. Specifically, from the highest law enforcement agency in the country.

“The election deniers are now ascendant in the federal government.”

“The election deniers are now ascendant in the federal government,” says Bellows, who spent eight years as the executive director of the Maine ACLU before assuming her current post. “These requests are not unlike the requests that the organizations they used to be affiliated with have asked for years.” But unlike conservative legal organizations, she adds, “the Department of Justice has the power to investigate, prosecute, and place people in jail.”

Riordan and Dhillon have been pursuing Maine's voter information since July, when the voting section of the DOJ's Civil Rights Division sent Bellows a letter requesting the state's unredacted registration list. Bellows wrote a careful response referencing federal court opinions and state statutes that preclude her from sharing the voter roll without appropriate redactions. In return, the DOJ sent her another threatening letter, followed by the ironically timed lawsuit on National Voter Registration Day.

Maine isn't the only state the DOJ contacted. Over the last six months, it has demanded full, unredacted voter rolls from dozens of states in an effort to create the federal government's first-ever national database of registered voters, accompanied by their private information: party affiliation, voting history, Social Security numbers, driver's license information, even physical characteristics. The DOJ has formally sued 14 states for the data so far, 12 of which are led by Democrats. (The sole exceptions are Vermont, which has a Republican governor but is otherwise deeply blue, and New Hampshire, where Republican Gov. Kelly Ayotte has publicly disagreed with President Donald Trump's plan to redraw congressional maps in advance of the midterms to give Republicans more seats.) Bellows believes Maine was among the first two states to be sued “because of animus”—also known as old-fashioned retribution.

The Justice Department already has tried to retaliate against Trump's political enemies, such as former FBI Director James Comey, who investigated ties between Russia and Trump's 2016 presidential campaign, and New York Attorney General Letitia James, who sued Trump over allegations that he inflated the value of his real estate holdings. (A federal judge recently dismissed both indictments, ruling that the prosecutor who brought the charges had been unlawfully appointed. The DOJ is reportedly weighing whether to re-indict them.) Bellows, though lesser known, is likely on the administration's radar for other reasons, too. Citing the 14th Amendment's clause barring officials who “engage in” insurrection from holding future office, she attempted to remove Trump from Maine's 2024 presidential ballot based on his connection to the January 6, 2021, attack on the US Capitol.

But Bellows, who is now running for governor, may not be the only one harmed by the DOJ data grab and the spurious claims supporting it. In 2024, crude analyses of voter roll data by right wingers led election officials in Waterford Township, Michigan, and Virginia to remove duly registered voters from the rolls.

So far, challenges like these have taken place on a much smaller scale: state by state or even county by county. The DOJ's current effort to assemble *every* state's voter data poses an exponentially larger threat to voting rights. More than a dozen state election officials, former DOJ staff, and election experts told *Mother Jones* that a national database of voter registration information could lead to massive data breaches of Americans' private information and reinforce false narratives about the frequency of voter fraud—narratives Trump and his allies could weaponize to challenge election outcomes. Worse yet, the bad data could give Republican-led states cover to illegally cull eligible voters from their rolls, stopping certain people from voting at all.

“These unprecedented demands for vast amounts of voter data are part of a larger pattern of actions indicating a reckless grab for power over American elections,” Bellows says.

It could also lead to a vast expansion of the number of citizens who appear on Trump’s hit list—one that, depending on your personal data, may soon include you.

0.65	51.24	-0.22	24.77	14.75	42.47	77.68
4.05	15.23	-0.08	6.45	4.82	20.20	-4.00
4.42	15.12	2.08	15.02	13.07	6.44	11.2

The right-wing campaign to weaponize the DOJ’s Civil Rights Division, which former Attorney General Eric Holder once called the “crown jewel” of the department, dates back more than two decades.

After the election of President George W. Bush in 2000, *National Review* called for a radical restructuring of the division. “There may be no part of the federal government where liberalism is more deeply entrenched,” wrote national correspondent John J. Miller. “Republicans should work to gain more control over the civil rights division and its renegade lawyers.”

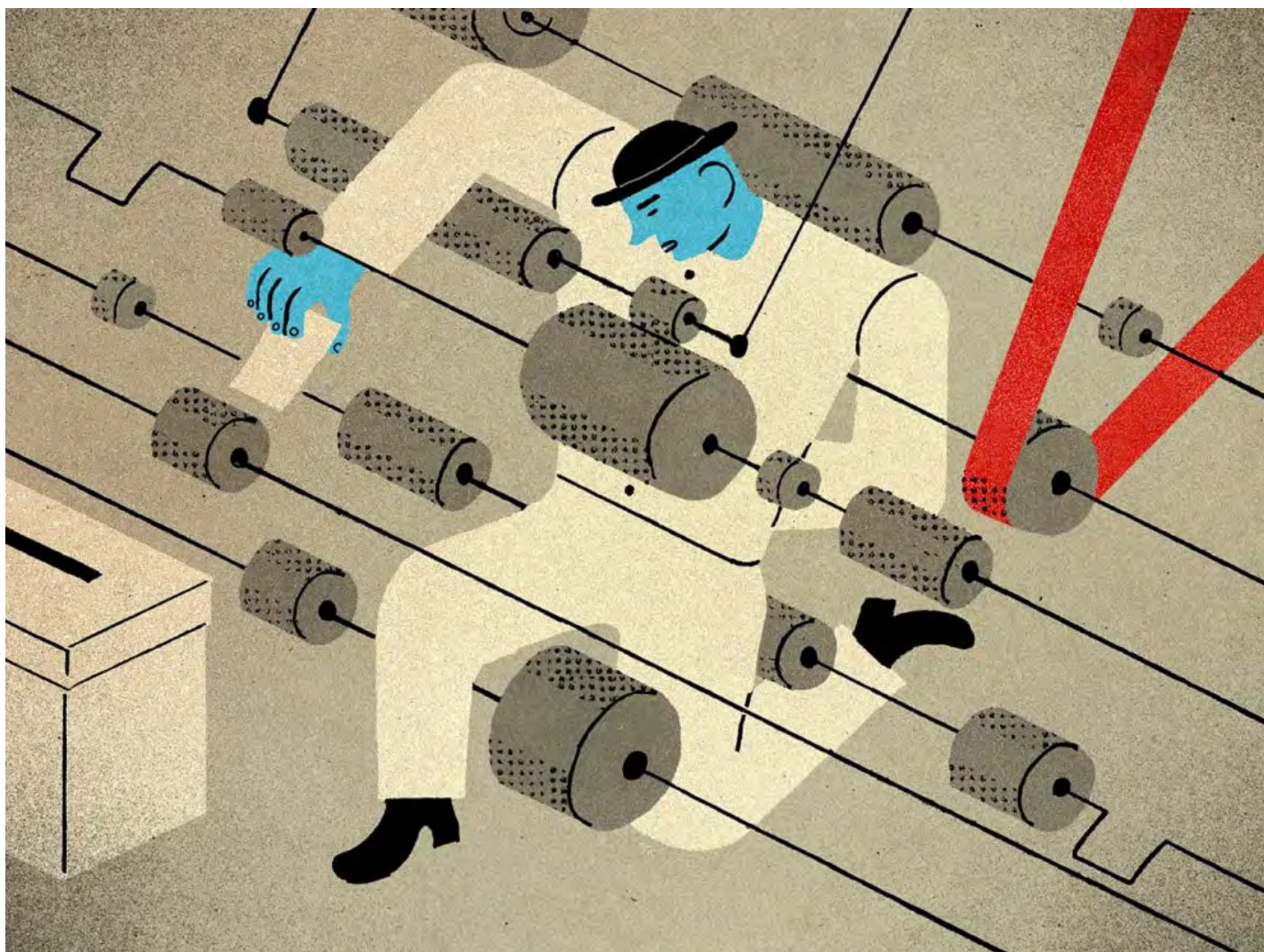
“My tentative plans are to gerrymander all of those crazy libs right out of the section.”

And a year later, that’s precisely what they did. Attorney General John Ashcroft tapped Brad Schlozman, a Kansas-based lawyer with no prior civil rights litigation experience, as deputy assistant attorney general for civil rights. His responsibilities included overseeing hiring and supervision for the division’s voting section, which enforces the Voting Rights Act and other federal voting laws. Schlozman did little to hide his disdain for the section he now led. “My tentative plans are to gerrymander all of those crazy libs right out of the section,” he wrote to a former colleague in July 2003.

Schlozman embarked on a hiring spree of what he called “RTAs,” short for “right-thinking Americans,” recruiting lawyers from the Federalist Society, the National Republican Lawyers Association, and the Bush-Cheney campaign. A joint investigation by the department’s inspector general and its Office of Professional Responsibility found that “virtually all of the attorneys (97 percent) hired by Schlozman whose political and ideological affiliations were evident in the hiring process were Republican or conservative.”

Veteran civil rights lawyers with decades of experience began leaving in droves, including the well-respected chief of the voting section, Joe Rich. Schlozman made Hans von Spakovsky, who had been among the first major figures in the GOP to push the myth of widespread voter fraud, de facto head of the section.

Soon, the department’s political appointees overruled career lawyers to approve GOP-backed laws that were regarded as racially discriminatory, including a mid-decade congressional redistricting plan in Texas that eliminated two majority-minority districts and a Georgia voter ID law that disproportionately harmed Black voters.



David Plunkert

“You take an oath to uphold the laws of the United States,” Robert Kengle, the deputy chief of the voting section from 1999 to 2005, told *Mother Jones*’ Ari Berman in his 2015 book, *Give Us the Ballot*. “These guys didn’t believe in the laws of the United States. They came in to work for an institution for which they had the utmost contempt.”

One of the attorneys hired by Schlozman was J. Christian Adams, a solo practitioner in Virginia who had served as a Bush-Cheney poll watcher in Florida. Rich described him as “Exhibit A of the type of people hired by Schlozman.”

Adams helped bring the DOJ’s first-ever Voting Rights Act case on behalf of white voters, who claimed they were discriminated against by the Black head of the local Democratic Party in Noxubee County, Mississippi. Career lawyers viewed it as a perversion of the law, which was intended to protect Black voters who were disenfranchised by segregationist whites in states like Mississippi.

By the end of the Bush administration in 2008, the DOJ’s inspector general found that Schlozman had violated federal law and committed misconduct by “improperly [considering] political and ideological affiliations in the recruitment and hiring of career attorneys in the Civil Rights Division.” But the anti-voting positions of the likes of von Spakovsky and Adams had already become institutionalized and were spreading within the GOP.

A couple of years later, in 2010, Adams loudly accused the Obama administration of anti-white bias when the DOJ dropped a case he spearheaded alleging that white voters were intimidated at the polls in Philadelphia by the New Black Panther Party. An internal review found no evidence of improper political interference, but by this point, Adams had resigned in protest. He would go on to become head of the right-wing legal group PILF in 2015. In addition to

filing lawsuits against local jurisdictions to force them to remove voters from their rolls, PILF published two reports in 2016 and 2017, “Alien Invasion in Virginia” and “Alien Invasion II,” that sought to validate Trump and his allies’ claims of widespread voter fraud by noncitizens.

The reports, which included names, addresses, and private information like Social Security numbers, claimed that more than 5,500 noncitizens had registered to vote in Virginia and 1,852 people had cast nearly 7,500 illegal ballots since the late 1980s. “This is the real foreign influence on American elections,” Adams told Fox News. “Foreigners are getting on American voter rolls and, as we documented, casting ballots by the thousands.”

PILF called on the Justice Department to bring felony charges against the voters it identified. Republican political activists drew up plans to post signs at polling places warning of voter fraud, which Adams said should be “in Spanish” to be “effective.”

It soon became clear, however, that PILF had relied on faulty methodology. As *Mother Jones* previously reported, “Alien Invasion II” spotlighted the “astonishing” example of one voter, Maureen Erickson, who listed a Guatemalan address on her registration form. “Ms. Erickson voted in 14 different elections—most recently in 2008—before her registration was canceled,” the report stated.

But it turned out that Erickson was a US citizen living in Guatemala as a missionary. “I think it is odd that they chose ‘Maureen Erickson’ as their poster child for voter fraud,” her husband, Todd Erickson, wrote in a letter to the *Washington Times* after it picked up the story. “There was obviously not much additional research done on the person that they held up as an example of this illegal activity.”

When Virginia election officials warned PILF that it was using unreliable data—such as targeting individuals who did not check a citizenship box at the DMV—to identify “suspected aliens,” PILF staffer Logan Churchwell agreed in an email to Adams that their concerns could “be true.” But this was an opportunity, Churchwell said, to “convert pushback into official confusion to justify our call for a top-down overhaul.”

“The fog of war favors the aggressor here,” added Churchwell, who remains research director at PILF.

In 2018, four Virginia voters whom PILF falsely accused of voting illegally filed a lawsuit against Adams and PILF, accusing them of violating the Voting Rights Act and the 1871 Ku Klux Klan Act—which empowers individuals to sue when vigilante groups threaten their 14th Amendment rights—through “a modern, covert, and particularly insidious method of voter intimidation.” PILF settled the case before it went to trial, with Adams agreeing to apologize to the plaintiffs and PILF pledging to redact sensitive personal information.

The reports should have been a cautionary tale about the dangers of overhyped fraud claims and the misuse of sensitive voter information, but Trump and his allies were undeterred and determined to spread such misinformation to a much bigger audience.

After claiming with no proof that he lost the popular vote in 2016 because 3 million people voted illegally, Trump brought back veterans of the Bush Justice Department, including Adams and von Spakovsky, as members of his Presidential Advisory Commission on Election Integrity. Von Spakovsky advised the commission to reprise the Schlozman-era playbook and exclude Democrats and “mainstream Republican officials and/or academics” from serving on it. He and Adams secretly advised Vice Chair Kris Kobach, then-Kansas secretary of state, on the commission’s first major action: a sweeping request for sensitive voter data from all 50 states, including party affiliation, voter history, and Social Security numbers. Kobach wrote that it would be “very helpful in the Commission’s work identifying fraudulent registrations and other forms of voter fraud.”

But the request, made in June 2017, infamously backfired. The Republican secretary of state of Mississippi, Delbert Hosemann, told the commission to “go jump in the Gulf of Mexico.” His GOP counterpart in Louisiana said the

“President’s Commission has quickly politicized its work by asking states for an incredible amount of voter data that I have, time and time again, refused to release.” Even Kobach, in his position as the top election official in Kansas, was unable to hand over voters’ Social Security numbers because they couldn’t be divulged by state law, nor could secretaries of state from Indiana, Maine, and New Hampshire, who also served on the commission. In the end, 21 states refused to provide any data, while the rest only partially complied.

The commission had tried to validate Trump’s fraud claims, but it disbanded after less than a year while facing at least eight lawsuits. A draft staff report of its findings included a section on “Evidence of Election Integrity and Voter Fraud Issues” that was, tellingly, left blank.

The commission’s failure should have put to bed the myth of widespread voter fraud once and for all—and prevented the federal government from ever again asking for such extensive information on voters. But Trump’s attempt to overturn the 2020 election convinced more of his supporters that elections were rigged, emboldening groups like PILF to turbocharge their efforts to restrict access to the ballot. In the runup to the 2024 election, Trump and his allies filed scores of lawsuits designed to make it harder to vote and easier to question election outcomes. PILF, along with the RNC and Harmeet Dhillon’s law firm, were at the forefront of this legal onslaught.

When Trump returned to the White House, an emboldened MAGA movement once again set its sights on transforming the DOJ’s Civil Rights Division and its voting section from a place that is entrusted with protecting people’s right to vote to one that jeopardizes it.

“This administration is abandoning the congressional mandate that the division has to stamp out discrimination and protect vulnerable populations,” says Chiraag Bains, who served as a high-ranking official in the Civil Rights Division from 2014 to 2017. “They’re not just abandoning it. They’re actually weaponizing the power of the federal government to try to cut off access to the ballot.”

0.65	51.26	-0.22	28.90	14.05	46.47	70.0
4.05	15.29	40.48	6.65	4.81	20.20	40.0
15.02	11.01	6.44	10.0			

A week after the 2024 election, Cleta Mitchell, a recent chair of PILF’s board (von Spakovsky is the current chair) and an attorney involved in Trump’s attempt to overturn the 2020 election, called on the administration to fire “every lawyer in the Voting Section and likely in the Civil Rights Division. They are not supportive of Pres Trump or MAGA. There has to be a reckoning.”

The now-reinvigorated wolves were back in the henhouse. Two days after the inauguration, the department’s political appointees ordered the Civil Rights Division to freeze work on all new cases. Shortly thereafter, former Florida Attorney General Pam Bondi, who had traveled to Pennsylvania in 2020 to amplify Trump’s false claims of voter fraud, was confirmed as US attorney general. The department put Mac Warner, a former West Virginia secretary of state who claimed that the CIA stole the 2020 election, in charge of the Civil Rights Division on an interim basis.

Over the winter and spring, the Trump DOJ began systematically withdrawing from voting rights cases filed under the Biden administration, refusing in nearly every instance to meet with the career attorneys who worked on them. “There was an utter lack of interest in what the day-to-day work of the voting section entailed,” says one former lawyer in the Civil Rights Division.

On March 31, when the department dropped a case challenging voting restrictions passed in Georgia in 2021, Bondi alleged that the Biden administration had “fabricated claims of false voter suppression.”

“The press release from the Georgia case was insulting to all the career lawyers who worked on it,” says another former DOJ lawyer. “To call something fraudulent from the institution you now lead was deeply troubling.”

Days later, the Senate confirmed Harmeet Dhillon, a Trump ally whose law firm had filed several lawsuits attacking voting rights, as head of the Civil Rights Division. Dhillon had amplified Trump’s false claims of fraud as a legal adviser to his 2020 campaign, calling on the Supreme Court to overturn the election results.

Dhillon removed the division’s longtime mandate of stopping racial discrimination in voting from the section’s mission statement and instead pledged to address Trump-inspired priorities that included “preventing illegal voting, fraud, and other forms of malfeasance and error.”

By the end of April, Trump’s appointees had dismissed every active case in the voting section and reassigned the section’s chief and five top managers to the obscure complaint adjudication office, the DOJ’s version of Siberia. Career attorneys who’d stayed during Trump’s first administration and thought they could survive Trump 2.0 decided to leave en masse. Just a few months in, more than 250 attorneys had departed the Civil Rights Division, 70 percent of the total staff, and the number of career attorneys in the voting section had shrunk from 30 to just three.

At the end of May, Maureen Riordan, who had been litigation counsel at PILF during the Biden years, took over as acting head of the voting section. A 20-year veteran of the DOJ who spent much of her career in the voting section, Riordan had resigned when Biden took office. At PILF, she had focused on filing lawsuits against various states, aimed at obtaining their voter roll information for the purpose of analyzing it for purported fraud.

When she returned to the DOJ under Trump, the department’s work had effectively become inseparable from the mission of the right-wing “election integrity” organizations whose leaders now staffed the new administration. With the MAGA takeover complete, the voting section launched its most audacious scheme yet, reprising the Trump administration’s demand for sensitive voter data from all 50 states. And this time, it would retaliate against those who refused to comply.

0.65	51.24	-0.22	28.29	14.05	46.67	70.8
4.05	15.29	40.48	15.82	13.09	6.44	40.9

A couple of weeks before the DOJ began demanding Maine’s voter rolls, PILF, Riordan’s old employer, sent its own letter to Bellows, alleging that its assessment of commercially available data and newspaper obituaries suggested there were more than 18,000 “apparently deceased” people on Maine’s voter rolls.

Responding to that previously unreported accusation, Bellows called its claim a “damned lie from an organization that cares more about conspiracy theories than election integrity.” Churchwell, from PILF, says their data collection methods have evolved since 2017 to prioritize credit data over other “cheap” commercial options: “We’ve raised the standard. Your experts are in the wailing and gnashing of teeth in outer darkness stage of their activism, and my heart goes out to them.”

For starters, every month, Maine’s 487 municipal election clerks review death records from the state’s vital records bureau and cancel the registrations of individuals who have died. As a fail-safe, Maine also compares its voter roll to the Social Security Administration’s Limited Access Death Master File at least once annually. Moreover, even if a deceased person’s name did appear on the voter roll for a short time, that does not mean a vote was illegally cast in their name.

This wasn’t the first time PILF made such a claim. The group sued Michigan in 2021, alleging that its assessment of publicly attainable data showed there were 25,000 dead voters on Michigan’s rolls. A federal judge dismissed the claim in March 2024. In May, the 6th US Circuit Court of Appeals rejected PILF’s argument a second time, concluding that

Michigan makes an “inherently rational, sensible attempt at maintaining accurate voter registration lists.” (In November, PILF asked the Supreme Court to reconsider the lower court’s decision.)

But PILF succeeded in advancing the voting fraud narrative—even if its lawsuit has so far failed. As is often the case, the rulings on the Michigan lawsuit didn’t get nearly as much attention as the claims that precipitated it. “Usually, sensational allegations of crimes go viral,” Bellows says, “and the less sensational finding that people are innocent often doesn’t have the same reach.”

Most of the lawsuits—whether from groups like PILF or the mightier Justice Department—allege violations of the National Voter Registration Act. Congress passed the 1993 bipartisan law with the intention of making it easier to register to vote. Dubbed the “Motor Voter Act,” the law simplified voter registration by making the process accessible at DMVs and other public agencies across the country. The law also included a provision to ensure that state voter rolls, which were anticipated to add new voters, were properly maintained. The US Constitution assigns the responsibility of managing elections to the states, and consequently, the act doesn’t tell states how exactly they should maintain their rolls; it merely says they should “conduct a general program that makes a reasonable effort to remove the names of ineligible voters.”

Bellows attests that Maine is doing just that. In February 2025, the state’s election division canceled 180,584 inactive voter registrations—the largest bulk removal in nearly 20 years. But the act’s open-ended language has provided an opening for election denialism crusaders, including the ones who now run the DOJ.

“Many election officials, including me, worry that the Trump administration wants this information so that it could be used to target, harass, and intimidate individual citizens.”

“These groups are trying to weaponize the law in a way that’s contrary to the purposes of the statute,” says Bains, the former DOJ Civil Rights Division official, now a senior fellow at the Brookings Institution. “Most of these lawsuits that we’re talking about are aimed at pursuing mass purges of exactly the nature that the statute was written to prevent.”

At least 40 states have received written requests from the Justice Department for their voter files, according to the Brennan Center for Justice. DOJ officials have said they eventually want the data from every state. So far, only two—Indiana and Wyoming—have complied, though the administration has adopted a harder stance in recent weeks. As of early December, the department has filed lawsuits against 14 states, beginning with Maine and Oregon.

“On the surface, it may seem like regular oversight, but it’s not,” Nevada Secretary of State Cisco Aguilar argued during a September press briefing with the States United Democracy Center, a group devoted to fair and secure elections. “The DOJ has the backing of the federal government. They’re trying to use the immense power to intimidate states into complying.”

At the same briefing, Michigan Secretary of State Jocelyn Benson outlined multiple ways the data demanded by the department could be used vindictively.

“Many election officials, including me, worry that the Trump administration wants this information so that it could be used to target, harass, and intimidate individual citizens, political adversaries, and potentially deter entire communities from voting,” Benson said. “It could also be used to pressure states to remove otherwise eligible citizens from the rolls based on pernicious or suspect information.”

Administration officials have yet to explain their reasons for trying to create a national voter roll, but the DOJ confirmed to *States Newsroom* that the data was “being screened for ineligible voter entries.”

The agency is working with the Department of Homeland Security to run voter information through Systematic Alien Verification for Entitlements, or SAVE, an online platform that provides access to various government databases in one place. Since its inception in 1987, the tool has been used to verify the citizenship of people applying for government benefits by checking alien identification numbers assigned to them by DHS. The Trump administration has dramatically expanded the tool in recent months, adding Social Security numbers and passport information to the system. As *Mother Jones* reported last month, DHS is also trying to connect every state's driver's license database to SAVE, so states can run their entire voter rolls through the database at one time. (A spokesperson for US Citizenship and Immigration Services, which administers SAVE, says states will need to ensure they are using the platform lawfully.)

The allegation that noncitizens are flooding state voter rolls is not supported by any data. One 2016 survey of 42 voting jurisdictions by the Brennan Center found just 30 cases of possible noncitizen voting out of nearly 24 million votes. Statistically, that's one ten-thousandth of 1 percent. Further, voter registration forms require Americans to affirm they are citizens, under penalty of perjury. The same form warns that those who lie could be fined, imprisoned, or deported. They'd also risk their future eligibility for citizenship. "To jeopardize that opportunity by voting just doesn't make sense," Nevada's Aguilar says.

While using SAVE to root out voter fraud is unlikely to turn up many—if any—noncitizen voters, the massive expansion of the program is likely to wrongly flag some American citizens as noncitizens, particularly naturalized citizens, newly married people who changed their last names, and people whose names don't match on their documents (for example, a man whose license says Nick but whose passport says Nicholas). A lawsuit filed by the League of Women Voters and the Electronic Privacy Information Center in September warned that DHS and the DOJ are "encouraging and enabling" states to search their voter rolls against SAVE, which the lawsuit alleges may culminate in some states "purging voter rolls."

In November, a federal judge agreed that the new use of SAVE was concerning: "The Court is troubled by the recent changes to SAVE and doubts the lawfulness of the Government's actions," wrote Judge Sparkle Sooknunan. However, she declined to block the administration from using it because the plaintiffs hadn't yet identified someone who had been directly harmed.

Even if the DOJ doesn't find any legitimate evidence of noncitizen voting, false matches would produce sensational headlines across the MAGA-verse, giving the administration more ammunition to undermine trust in elections.

"My guess is they want the voter files to be able to say we have the voter files, and we know there are X or Y fraudulent people on it," says Justin Levitt, who served as deputy assistant attorney general in the DOJ's Civil Rights Division under President Barack Obama. "It will be fiction, but now they'll say it because they have them. Even if they find an infinitesimal number of wrong people on the rolls, they will lie about the numbers."

The DOJ declined to comment for this story.

Beyond the possibility of voters being disenfranchised, the League of Women Voters and EPIC argue that every person's federal right to privacy would be encroached by the DOJ and DHS sharing data among themselves and state governments. Congress passed the Privacy Act of 1974 specifically to prevent the federal government from creating "formal or de facto national data banks" or "centralized Federal information systems" that would integrate the personal data of Americans stored at separate agencies, the lawsuit points out.

Add to all this the fact that a national voter file could also be a gold mine for hackers, especially as the Trump administration dismantles efforts to combat foreign and domestic election interference.

"The danger is once you compile all this information, then hackers only have to go to one place instead of going to all 50-plus jurisdictions that run elections," says Eileen O'Connor, who worked in the DOJ's voting section for nearly a

decade, including during Trump's first term. "It's just a hacker's dream to have all of this private, sensitive information collected somewhere."

In its efforts to inspect state voter rolls, the DOJ is also, evidently, considering sharing Americans' personal data with outside election denial groups. Rick Richards, a retired physician from Georgia with no experience as an election official, has met with Riordan and marketed his mass voter registration challenge system called EagleAI, which he helped develop with Cleta Mitchell's support, to the DOJ.

"We demonstrated the software to the DOJ. They like it. They would like to use it. Apparently, we can get data they can't," he said during a meeting hosted by Mitchell's group, the Election Integrity Network, according to a transcript obtained by *Mother Jones*. "I am in conversation with them about letting us have a task, a federal task, to bring their data into what we're doing and then be able to use the federal data, SAVE data, Social Security data, other data in here as well."

Despite its name, EagleAI uses no artificial intelligence. Like PILF, EagleAI relies on incomplete information, such as self-reported address changes registered with the US Postal Service and datasets purchased from private entities like utilities, credit card companies, or magazine publishers. Richards boasted on the same call that EagleAI flagged more than 50 percent of Fulton County, Georgia, voter registrations as "potential problems"—an indication of the system's dubious accuracy.

Had the right-wing election integrity skeptics behind EagleAI actually believed the county's voter roll was teeming with fraudulently registered voters, they likely would have presented these concerns to local officials. But according to Nadine Williams, Fulton County's director of registration and elections, that hasn't happened; her voter roll is audited monthly using verified data sources, and she's never heard from EagleAI, which she called an "unverified third-party group."

In response to questions from *Mother Jones*, Richards claimed that "the EagleAI Network program no longer exists," even though his email signature still includes that affiliation and the group's data was used to challenge more than 900 voters in New Jersey as recently as a month ago.

If the DOJ takes up Richards on his offer to use EagleAI on state voter rolls the department is suing to collect, it wouldn't be the first time Riordan has worked at a place that relies on faulty data to spread questionable conclusions about voter fraud.


Normally, the DOJ's voting section would work to prevent these kinds of efforts from affecting Americans' ability to vote. Now, the voting section itself is in on the effort. "The main activity the section seems to be engaged in at this point," says Levitt, the former deputy assistant attorney general, "is something illegal."

KEEP US RELENTLESS, INDEPENDENT, AND FREE TO READ.

For 50 years, *Mother Jones* has offered **honest, investigative reporting** you can rely on:

- **Relentless in the pursuit of truth**, unafraid to hold the powerful to account
- **Independent from influence or agenda** from oligarchs and corporations
- **Freely accessible to every reader**, never behind a paywall

But we can't do any of this without you. Reader support powers our newsroom to stay nimble and fearless, ready for whatever story comes next. If you can, **make a donation today.**


One-Time		Monthly	
\$	\$	\$	
Other Amount			
Continue			
			

KEEP US RELENTLESS, INDEPENDENT, AND FREE TO READ.

For 50 years, *Mother Jones* has offered **honest, investigative reporting** you can rely on:

- **Relentless in the pursuit of truth**, unafraid to hold the powerful to account
- **Independent from influence or agenda** from oligarchs and corporations
- **Freely accessible to every reader**, never behind a paywall

But we can't do any of this without you. Reader support powers our newsroom to stay nimble and fearless, ready for whatever story comes next. If you can, **make a donation today.**

One-Time		Monthly	
\$12	\$15	\$25	
Other Amount			
Continue			
			

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Copyright © 2026 Mother Jones and the Center for Investigative Reporting. All Rights Reserved.

Exhibit 9



Kris Warner
Secretary of State
State of West Virginia

1900 Kanawha Blvd. E.
Building 1, Suite 157K
Charleston, West Virginia 25305

Telephone: (304) 558-6000
Toll Free: 1-866-SOS-VOTE
Fax: (304) 558-0900
www.wvsos.gov

February 11, 2026

Via U.S. Mail & E-mail

Eric Neff
Acting Chief
Civil Rights Division, Voting Section
Department of Justice
150 M St. NE, Ste. 8-1807
Washington, DC 20002
Eric.Neff@usdoj.gov

Dear Mr. Neff:

The Office of the West Virginia Secretary of State ("WVSOS") acknowledges receipt of your February 4, 2026, correspondence, wherein the U.S. Department of Justice ("DOJ") requests confirmation that the position expressed in our September 22, 2025, letter remains our position on this matter.

For context, on September 8, 2025, the DOJ demanded that the WVSOS provide an electronic, unredacted copy of West Virginia's statewide voter registration list. The DOJ's request states that the list must include, among other data fields, the voter registrant's full name, date of birth, residential address, and either the individual's state driver's license number or the last four digits of the registrant's Social Security number, as required under the Help America Vote Act ("HAVA") for individuals registering to vote in federal elections. *See* 52 U.S.C. § 20901, *et seq.*

The DOJ cited various legal authorities supporting this request, including provisions of HAVA; the National Voter Registration Act of 1993 ("NVRA"), 52 U.S.C. § 20501, *et seq.*; Title III of the Civil Rights Act of 1960 ("CRA"), 52 U.S.C. § 20701, *et seq.*; and The Privacy Act of 1974, 5 U.S.C. § 552a.

Prior to responding to the DOJ's original request, our Office performed a thorough review of the cited statutes, none of which require compliance with such a broad request.

As set forth in the DOJ's September 8, 2025, letter, the stated purpose of the request is to "assess your state's compliance with the statewide [voter registration list maintenance] provisions of the NVRA." However, the demand included only a vague explanation of the basis and specific purpose of the request.

Based on recent verbal communications with your office, the alleged purpose of the DOJ's request is to run West Virginia's entire voter list through the Systematic Alien Verification for Entitlements ("SAVE") database, which is administered by the U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, Verification Division.

However, as we discussed, the WVSOS is a registered and recently approved user of the SAVE database. Despite this fact, and despite our offer to work collaboratively with the DOJ to utilize the SAVE database within the confines of federal and state law, the DOJ has restated its position that, under the CRA, it is entitled to the unredacted voter information of West Virginia citizens.

As set forth in our September 22, 2025, correspondence, West Virginia law protects the sensitive personally identifiable information of its voters, and the Secretary of State takes seriously his responsibility to safeguard such information from unauthorized disclosure. Nothing in the interim has altered our position.

The CRA, NVRA, and HAVA were enacted by Congress to protect voting rights. Congress places responsibility on the states to administer voter registration and elections in accordance with these statutes. To that end, West Virginia has enacted a series of statutes governing voter list maintenance. *See* W. Va. Code § 3-2-1, *et seq.* A summary of West Virginia's voter registration list maintenance procedures and data sources was included in our original letter.

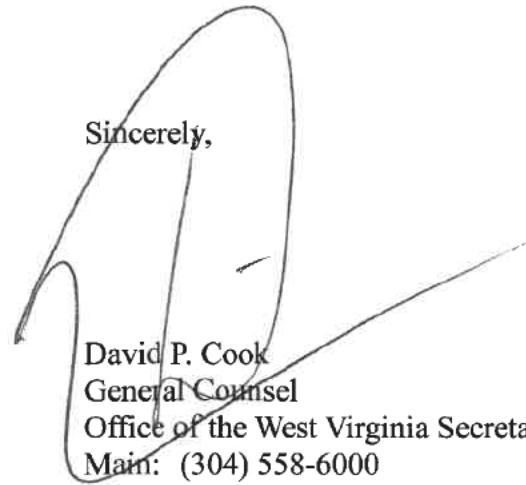
At present, West Virginia has 1,195,305 registered voters. Since 2017, 408,397 voter registration records have been lawfully cancelled, 62,756 of which were cancelled under Secretary of State Kris Warner's administration. Nevertheless, to further assist your inquiry, we remain willing to provide a detailed narrative of our voter list maintenance procedures upon request.

W. Va. Code § 3-2-30(a) provides that any person may examine the voter registration records of West Virginia residents. However, the statute expressly prohibits the disclosure of a registrant's Social Security number or driver's license number. Further, the Privacy Act of 1974 provides that executive agencies may not collect personal or sensitive information from a West Virginia citizen exercising his or her constitutionally protected right to vote absent applicable statutory authority. No such exception exists under the CRA, NVRA, HAVA, or the Privacy Act of 1974.

The Secretary of State respects your position in this matter and remains willing to work with the DOJ to reach an amicable resolution within the limits of state and federal law. As set forth in our prior correspondence, the WVSOS makes voter registration lists available subject to the statutory limitations set forth above.

Please do not hesitate to contact me with any questions or concerns.

Sincerely,

A large, stylized handwritten signature in black ink, appearing to read 'D. Cook', is written over the typed name and title.

David P. Cook
General Counsel
Office of the West Virginia Secretary of State
Main: (304) 558-6000
Email: DCook@wvsos.gov

Exhibit 10

SUPPLEMENTARY INFORMATION: The Commission instituted this investigation on January 24, 2003, based on a complaint filed by Charles D. Walkden ("Walkden") of Homer, Alaska. 68 FR 3550 (2003). The complaint, as amended, alleged violations of section 337 in the importation, sale for importation, and sale within the United States after importation of certain truck bed ramps and components thereof that infringe claim 1 of U.S. Patent No. 5,795,125 ("the '125 patent"). The Commission named as respondents ETEC of Saskatoon, SK, Canada; Textron Inc. ("Textron") of Providence, Rhode Island; VIP Distributing of Anchorage, Alaska; Southwest Distributing Co. of Clinton, Oklahoma; and Hamilton Equipment Inc. of Ephrata, Pennsylvania. *Id.* Textron was subsequently terminated from the investigation on the basis of a consent order.

On June 2, 2003, the Commission investigative attorney ("IA") moved pursuant to Commission rule 210.15(a) for summary determination of non-infringement. On July 10, 2003, the ALJ issued an ID granting the IA's motion. No petitions for review of the ID were filed.

This action is taken under the authority of section 337 of the Tariff Act of 1930, as amended (19 U.S.C. 1337), and 210.42 of the Commission's Rules of Practice and Procedure (19 CFR 210.42).

Issued: August 6, 2003.

By order of the Commission.

Marilyn R. Abbott,

Secretary to the Commission.

[FR Doc. 03-20384 Filed 8-8-03; 8:45 am]

BILLING CODE 7020-02-P

DEPARTMENT OF JUSTICE

[AAG/A Order No. 015-2003]

Privacy Act of 1974; Systems of Records

Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), the Department proposes to modify the following Privacy Act systems of records:

Central Civil Rights Division Index File and Associated Records, JUSTICE/CRT-001 (previously published on February 20, 1998, at 63 FR 8659);

Civil Rights Case Load Evaluation System—Time Reporting System, JUSTICE/CRT-003 (previously published on October 17, 1988, at 53 FR 40510);

Registry of Names of Interested Persons Desiring Notifications of Submissions Under Section 5 of the Voting Rights Act, JUSTICE/CRT-004

(previously published on October 17, 1988, at 53 FR 40511);

Files on Employment Civil Rights Matters from Persons Outside of the Department of Justice, JUSTICE/CRT-007 (previously published on October 17, 1988, at 53 FR 40512); and Civil Rights Division Travel Reports, JUSTICE/CRT-009 (previously published on October 17, 1988, at 53 FR 40514).

The Department is publishing modifications to the above systems of records. This notice includes some major changes such as adding new routine uses. Also, the Department made other non-substantive changes in all the above systems to provide clarification, such as to correct typographical errors, to provide updated addresses, to update information on particular statutes, to clarify existing routine uses, to add data elements omitted from previous notices, and to reflect nomenclature changes. The proposed rule for the Privacy Act exemptions is also being updated and is published in today's **Federal Register**.

First, in the Central Civil Rights Division Index File and Associated Records system, CRT-001, the Department proposes to allow records which may disclose a violation or potential violations of law to be referred to the appropriate authority charged with the responsibility for investigation, enforcing or prosecuting such violation. Two other routine use disclosures permit the disclosure of information regarding the progress and results of investigations to contractors, experts, students, consultants, mediators, negotiators, and other persons performing work or on assignment to the Federal Government. Another routine use will permit the disclosure of information to former employees of the Department for matters in which they were involved. In addition, a revised routine use will permit disclosure of health care-related information obtained during health care-related investigations.

Second, the Department proposes to add five routine use disclosures to Civil Rights Interactive Case Management System, CRT-003. The first routine use allows records which may disclose a violation or potential violations of law to be referred to the appropriate authority charged with the responsibility for investigation, enforcing or prosecuting such violation. Two routine uses are similar to those above: To permit the disclosure of information regarding the progress and results of investigations to contractors, experts, students, consultants, and other persons performing work or on

assignment to the Federal Government; and to permit the disclosure of information to former employees of the Department for matters in which they were involved. One routine use will permit disclosure to complainants and victims to provide information about the progress and/or results of an investigation or case. Further, information may be disclosed to the media under certain circumstances unless it would constitute an unwarranted invasion of personal privacy.

Third, the Department proposes to add three routine use disclosures to Registry of Names of Interested Persons Desiring Notifications of Submissions Under Section 5 of the Voting Rights Act, CRT-004. Two routine uses are similar to that above: To permit the disclosure of information regarding the progress and results of investigations to contractors, experts, students, consultants, and other persons performing work or on assignment to the Federal Government; and to permit the disclosure of information to former employees of the Department for matters in which they were involved. Another routine use will allow records which may disclose a violation or potential violations of law to be referred to the appropriate authority charged with the responsibility for investigation, enforcing or prosecuting such violation.

Fourth, the Department proposes to add three routine use disclosures to Files on Employment Civil Rights Matters from Persons Outside of the Department of Justice, CRT-007. This routine use will permit the disclosure to complainants and victims to provide information about the progress or results of an investigation or case. Two routine uses are identical to that above: To permit the disclosure of information regarding the progress and results of investigations to contractors, experts, students, consultants, and other persons performing work or on assignment to the Federal Government; and to permit the disclosure of information to former employees of the Department for matters in which they were involved. One routine use will permit disclosure to complainants and victims to provide information about the progress or results of an investigation or case.

Fifth, the Department proposes to add two identical routine uses as those above, for disclosure to contractors and former employees, in Civil Rights Division Travel Reports, CRT-009. The other routine use will allow records which may disclose a violation or potential violations of law to be referred to the appropriate authority charged with the responsibility for investigation,

enforcing or prosecuting such violation or law.

In addition, the Civil Rights Division has one system of records, CRT-002, Files of Application for the Position of Attorney with the Civil Rights Division, which is now covered by two government wide systems of records of the Office of Personnel Management (OPM): OPM/GOVT-1, General Personnel Records; and OPM/GOVT-5, Recruiting, Examining and Placement Records (both published on April 27, 2000, at 65 FR 24732-24753). Accordingly, these government wide system notices replace, and the Department hereby removes, on the effective date of this notice, the following notice previously published by an individual Department of Justice component:

Files of Application for the Position of Attorney with the Civil Rights Division, JUSTICE/CRT-002 (previously published on December 17, 1985, at 50 FR 51482).

Finally, the Office of Special Counsel for Immigration Related Unfair Employment Practices was merged into the Civil Rights Division, and its two remaining systems of records are being incorporated into the Civil Rights Division's systems of records. Accordingly, this system notice replaces, and the Department hereby removes, on the effective date of this notice, the following notices previously published by individual Department of Justice components:

Office of Special Counsel, "Central Index File and Associated Records," OSC-001 (previously published on October 17, 1988, at 53 FR 40531); and Office of Special Counsel, "Special Counsel for Immigration Related Unfair Employment Practices Travel Reports," OSC-003 (previously published on September 15, 1988 at 53 FR 35926).

The Office of Special Counsel's systems of records, OSC-001 and OSC-003, were incorporated into the Civil Rights Division's systems of records, CRT-001 and CRT-009, respectively.

The modified systems of records are printed below.

In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment; and the Office of Management and Budget (OMB), which has oversight responsibility of the Act, requires a 40-day period in which to conclude its review of the system. Therefore, please submit any comments by September 10, 2003. The public, OMB and the Congress are invited to submit comments to: Mary Cahill, Management and Planning Staff, Justice Management Division, Department of Justice, 1331

Pennsylvania Ave., NW., Washington, DC 20530 (1400 National Place Building).

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress.

Dated: July 24, 2003.

Paul R. Cortis,
Assistant Attorney General for Administration.

JUSTICE/CRT-001

SYSTEM NAME:

Central Civil Rights Division Index File and Associated Records, CRT-001.

SYSTEM LOCATION:

United States Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

These persons may include: Subjects of investigations, victims, potential witnesses, individuals of Japanese ancestry who were eligible, or potentially eligible, for restitution benefits as a result of their evacuation, relocation, or internment during World War II, and representatives on behalf of individuals and other correspondents on subjects directed or referred to CRT or other persons or organizations referred to CRT in potential or actual cases and matters of concern to CRT, and CRT employees who handle complaints, cases or matters of concern to CRT.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system consist of case files, matters, memoranda, correspondence, studies, and reports relating to enforcement of civil rights laws and other various duties of the Civil Rights Division. The delegated legal duties and responsibilities of each section are described in detail at the Civil Rights Division Web page: <http://www.usdoj.gov/crt/crt-home.html>. In addition to the sections, the Civil Rights Division maintains records related to the duties of the former Office of Redress Administration pertaining to the identification, location and authorization for restitution payments to eligible individuals of Japanese ancestry who were evacuated, relocated or interned during World War II. These restitution payments were authorized by section 105 of the Civil Liberties Act of 1988 (50 U.S.C. App. 1989b). Finally, the names of some individuals, e.g., witnesses, may not yet be on the central indices and may be obtained by direct access to the file jackets. Such file jackets are located within the respective

sections of CRT according to the legal subject matter assigned to each CRT section.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The records in the system of records are kept under the authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibility assigned to CRT under the provisions of 28 CFR 0.50, 0.51.

PURPOSES:

The purposes of this system are to assist all the sections within the Division in maintaining names of Division employees and their case investigation assignments, names of defendants or investigation targets, victims, witnesses or potential witnesses, or other persons or organizations as they relate to potential or actual cases, investigations, and matters of concern to CRT. Other purposes are to assist employees and officials within the Division to review and make decisions in the course of investigations and legal proceedings, to assist the Division in preparing budget requests, to respond to inquiries from outside the Department, and to carry out other authorized Department functions.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or Tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(2) In the course of the administration by CRT of a federally mandated program, or the investigation or litigation of a case or matter, a record may be disseminated to a Federal, State or local agency, or to an individual or organization, if there is reason to believe that such agency, individual or organization possesses information or has the expertise in an official or technical capacity to assist in the administration of such program or to analyze information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such assistance, information or expert analysis, or to obtain the

cooperation of a prospective witness or informant;

(3) A record relating to a case or matter, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(4) A record relating to a case or matter may be disseminated to an actual or potential party to litigation or the party's attorney (a) for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or (b) in informal discovery proceedings;

(5) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any determination that has been made;

(6) A record relating to a person held in custody or probation during a criminal proceeding or after conviction may be disseminated to any agency or individual having responsibility for the maintenance, supervision or release of such person;

(7) A record may be disseminated to the United States Commission on Civil Rights in response to its request and pursuant to 42 U.S.C. 1975d;

(8) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(9) A record may be disseminated to mediators, negotiators or other persons engaged in efforts to resolve or settle cases or matters pending in the Division as is necessary to enable them to perform their assigned duties;

(10) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim;

(11) Information relating to health care fraud may be disclosed to private health plans, or associations of private health plans, health insurers, or associations of health insurers, to

promote the coordination of efforts to prevent, detect, investigate, and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals, which have jurisdiction over claims against private health plans for allegedly improper disclosures to the Department of Justice of information concerning suspected health care fraud, in determining whether the private health plan qualifies for statutory immunity from civil liability as provided by Section 201 of the Health Insurance Portability and Accountability Act of 1998, codified at 42 U.S.C. 1320a-7c(a)(3)(B)(iii);

(12) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(13) Information may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituent who are subjects of CRT records;

(14) A record may be disclosed as a routine use to the National Archives and Records Administration (NARA) and to the General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(15) To a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Information in this system is stored on index cards, in file jackets, and on computer disks or tapes.

RETRIEVABILITY:

Records are retrieved by the names of individuals or by case numbers assigned to certain cases being investigated by the Department.

SAFEGUARDS:

Information in manual and computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

RETENTION AND DISPOSAL:

Records are maintained on the system while current and required for official Government use. When no longer needed on an active basis, the paper files are transferred to the Federal Records Center, Suitland, Maryland and some records are transferred to computer tape and stored in accordance with Department security regulations for systems of records. Final disposition is in accordance with records retention schedules approved by NARA.

SYSTEM MANAGER(S) AND ADDRESS:

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

NOTIFICATION PROCEDURE:

Part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(2) and (k)(2). Address inquiries to the System Manager listed above.

RECORD ACCESS PROCEDURES:

Part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(2) and (k)(2). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record retrievable in this system shall be made in writing, with the envelope and letter clearly marked "Privacy Access Request." Include in the request the full name of the individual, his or her current address, date and place of birth, notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), the subject of the case or matter as described under "Categories of records in the system," and any other information which is known and may be of assistance in locating the record, such as the name of the civil rights related case or matter involved, where and when it occurred and the name of the judicial district involved. The requester will also provide a return address for

transmitting the information. Access requests should be directed to the System Manager listed above.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend non-exempt information retrievable in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Sources of information contained in this system may be an agency or person who has or offers information related to the law enforcement responsibilities and/or other statutorily-mandated duties of CRT.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted parts of this system from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the **Federal Register**. These exemptions apply only to the extent that information in a record pertaining to a particular individual relates to an official federal investigation and/or law enforcement matter. Those files indexed under an individual's name which concern only the administrative management of restitution payments under section 105 of the Civil Liberties Act of 1988 are not being exempted pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

JUSTICE/CRT-003

SYSTEM NAME:

Civil Rights Interactive Case Management System (ICM).

SYSTEM LOCATION:

United States Department of Justice, Civil Rights Division (CRT), 950 Constitution Ave., NW., Washington, DC 20530-0001.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

These persons may include: Complainants, victims, defendants, parties, experts, mediators, Assistant U.S. Attorneys, judges, and individuals or representatives on behalf of individuals in potential or actual cases and matters of concern under jurisdiction of the Civil Rights Division; and CRT employees, including

attorneys, paralegals, and professional staff, who handle complaints, cases or matters of concern to CRT.

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Records in this system pertain to a broad variety of cases and matters under the jurisdiction of the CRT relating to disability rights, education, employment, housing, special litigation, voting, criminal, enforcement, and other civil rights laws or matters;

(2) Summary information of these cases or matters is maintained in the system including such information as names of principal parties or subjects, proper case name, case numbers, judicial district, assignments, alleged violation, section of CRT responsible for the matter, and case status, ranging from the preliminary development stage, through investigation, litigation, compliance, appeal, conviction or closure; and

(3) The ICM also has a time reporting system that allows the CRT to capture, analyze and report the professional time attorneys, paralegals and other employees of the Division spend on investigation and case related tasks.

PURPOSE(S):

The ICM is designed to track, count and measure all investigations and cases throughout their life cycle. The CRT uses reports generated from this system to provide a profile for each section's activities and to furnish management with a global perspective to the CRT workload. The ICM also has a time reporting system that allows the CRT to capture, analyze and report the level of effort attorneys, paralegals, and professional staff spend on investigation and case related tasks. One purpose of this system is to assist employees and officials of the Department to keep track of resources and professional time devoted to individual assignments to matters and broad categories of cases. Another purpose is to assist the CRT in preparing budget requests and other reports which may be submitted to the Attorney General or to Congress.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The records in this system are kept under the authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be

disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or Tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(3) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or in informal discovery proceedings;

(4) A record may be disseminated to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(5) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim;

(6) A record may be disseminated to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(7) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available unless it is determined

that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(8) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records; and

(9) A record from the system or records may be disclosed to National Archives and Records Administration (NARA) and General Services Administration (GSA) for records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained electronically in the ICM computerized information system.

RETRIEVABILITY:

Information is retrieved by name or other identifier assigned to an individual.

SAFEGUARDS:

Information contained in the system is unclassified. It is safeguarded and protected in accordance with Departmental security regulations for systems or records. Access to the records is limited to those employees whose official duties require such access in order to perform their duties.

RETENTION AND DISPOSAL:

Records are maintained in the system while current and required for official Government use. When no longer needed on an active basis, the records are stored in accordance with Departmental security regulations for systems of records. The disposition schedule is pending approval at NARA.

SYSTEM MANAGER(S) AND ADDRESS:

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

NOTIFICATION PROCEDURE:

Address inquiries to the system manager listed above.

RECORD ACCESS PROCEDURE:

A request for access to a record retrievable in this system shall be made in writing, with the envelope and letter clearly marked "Privacy Access Request." Include in the request the full name of the individual involved, his or her current address, date and place of

birth, and notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), and any other information which is known and may be of assistance in locating the record. The requester should provide a return address for transmitting the information. Access requests should be directed to the System Manager listed above.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend their records should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Information on time-allocation is provided by CRT attorneys, paralegals and professional staff who handle complaints, cases or matters of concern to the CRT. Sources of information contained in this system are those records reflecting all cases or matters under consideration by CRT.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

JUSTICE/CRT-004

SYSTEM NAME:

Registry of Names of Interested Persons Desiring Notification of Submissions under Section 5 of the Voting Rights Act.

SYSTEM LOCATION:

U.S. Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons who have requested that the Attorney General send them notice of submissions under Section 5 of the Voting Rights Act of 1965, 42 U.S.C. 1973c.

CATEGORIES OF RECORDS IN THE SYSTEM:

The Registry contains the name, address and telephone numbers of interested parties, and, where appropriate, the voting area or areas with respect to which notification was requested by such persons.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

46 FR 877 (1981) codified in 28 CFR part 51, 42 U.S.C. 1973c, 5 U.S.C. 301 and 28 U.S.C. 509, 510.

PURPOSE(S):

The purpose is to maintain records in a Registry to identify persons interested

in receiving notification of submissions under Section 5 of the Voting Rights Act and to comply with their requests. Section 5, which applies to several states and some counties, requires that any change with respect to voting that a specially covered jurisdiction makes is legally unenforceable unless and until the jurisdiction obtains from the Federal court in the District of Columbia or from the Attorney General a determination that the change is not discriminatory on account of race, color, or membership in a language minority group. If the jurisdiction is unable to prove the absence of discrimination, the Attorney General objects to the change, and it remains legally unenforceable. Further, the Registry may be used to notify the persons listed therein of any proposed changes in the "Procedures for the Administration of Section 5 of the Voting Rights Act of 1965," 46 FR 870 (1981), codified in 28 CFR part 51, and to solicit their comments with respect to any such proposed changes.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or in informal discovery proceedings.

(3) A record may be disseminated to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from

the matters of which the complainants or victims complained or of which they were a victim;

(5) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(6) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(7) A record from a system of records may be disclosed as a routine use to National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(8) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility; and

(9) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, foreign, or tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Names are stored in a card file system, and an automated addresser.

RETRIEVABILITY:

Records in this system are retrievable by the names of interested persons or organizations.

SAFEGUARDS:

Information in the system is safeguarded in accordance with

Departmental rules and procedures governing access, production and disclosure of any materials contained in its official files.

RETENTION AND DISPOSAL:

An individual or organizational name is retained in the Registry until such time as that person or organization requests that the name be deleted.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Voting Section, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

NOTIFICATION PROCEDURE:

Address inquiries to: Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

RECORD ACCESS PROCEDURES:

This system contains no information about any individual other than as described in Categories of Records above. Persons whose names appear on the Registry may have access thereto or have their names and other information pertaining to them deleted or modified upon a request of the same nature as indicated in 46 FR 877 (1981), codified in 28 CFR part 51.

CONTESTING RECORD PROCEDURES:

Same as the above.

RECORD SOURCE CATEGORIES:

Sources of information in the Registry are those persons or organizations whose names appear therein by virtue of their having requested inclusion in the Registry pursuant to 46 FR 877 (1981), codified in 28 CFR 51.32.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

JUSTICE/CRT-007

SYSTEM NAME:

Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission.

SYSTEM LOCATION:

U.S. Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue NW., Washington, DC 20530-0001.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons seeking employment or employed by a state or a political subdivision of a state who have filed charges alleging discrimination in employment with the Equal Employment Opportunity Commission

(hereinafter EEOC) which have resulted in a determination by EEOC that there is probable cause to believe that such discrimination has occurred, and attempts by EEOC at conciliation have failed.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system may contain copies of charges filed with EEOC, copies of EEOC's "determination" letters, letters of transmittal from and to EEOC, analyses or evaluations summarizing the charge and other materials in the EEOC file, internal memoranda, attorney notes, and copies of "right to sue" letters issued by CRT. The system may also contain charges related to allegations of employment discrimination by public employers filed by individual complainants which have been referred to the Department of Justice by EEOC pursuant to 42 U.S.C. 2000e-5(f) (1) or 5(f) (2), or to allegations of a pattern or practice of violations of the Equal Employment Opportunity Act by a public employer which have been referred to the Department of Justice by EEOC pursuant to 42 U.S.C. 2000e-6. If the Department has determined to initiate an investigation or litigate a matter referred by EEOC the records pertaining to that matter are not contained in the system. Such records and their routine uses are described under the notice for the system named: Central CRT Index File and Associated Records/CRT-001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The records in this system of records are kept under authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

PURPOSE(S):

One purpose of this system is to assist employees and officials of the Department to make decisions regarding the issuance of right to sue letters or make decisions regarding prosecutions of alleged instances of employment discrimination. Another purpose is to assist the Division in preparing budget requests, statistical reports, and other internal functions of the Department.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) A record relating to this system, or any facts derived therefrom may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is

authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or in informal discovery proceedings;

(3) A record may be disseminated to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim;

(5) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(6) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(7) A record from a system of records may be disclosed as a routine use to National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906; and

(8) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee

regarding a matter within that person's former area of responsibility.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Information in the systems is stored on index cards, in file jackets, and in computer disks which are maintained by the Employment Litigation Section, Civil Rights Division.

RETRIEVABILITY:

Information is retrieved primarily by using the appropriate Department of Justice file number, or the name of the charging party, or the state in which the alleged discrimination occurred or through other logical queries to the computer based system.

SAFEGUARDS:

Information in manual and computer form is safeguarded and protected in accordance with applicable Departmental security regulations for systems of records. Staff members who are assigned a specific identification code will be able to use the computer or to access the stored information in order to perform their official duties.

RETENTION AND DISPOSAL:

If the Department determines not to prosecute a matter referred by the EEOC, the records transmitted with the referral are returned to the EEOC. Other records in the system are kept for routine use by the Department and when no longer needed are sent to the Federal Records Center or are destroyed. Records are retained and disposed of in accordance with item 25 of the General Records Schedule 1 as approved by the Archivist of the United States.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

NOTIFICATION PROCEDURE:

Same as the above.

RECORD ACCESS PROCEDURE:

A request for access to a record from this system shall be made in writing with the envelope and letter clearly marked "Privacy Access Request." The request should indicate the state where the alleged employment discrimination took place and the employer to which the charge was related. The requester should also provide the full name of the individual involved, his or her current address, date and place of birth, notarized signature or dated signature submitted under penalty of perjury (28

CFR 16.41(d)), any other known information which may be of assistance in locating the record, and a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Disclosure of part of the material in this system may be prohibited by 42 U.S.C. 2000e-5(b), 42 U.S.C. 2000e-8(e) and 44 U.S.C. 3510(b). Part of this system is exempted from access and contest under 5 U.S.C. 552a(k) (2).

RECORD SOURCE CATEGORIES:

Sources of information in this system are charging parties, information compiled and maintained by EEOC, and employees and officials of the Department of Justice responsible for the disposition of the referral request.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted the system from 5 U.S.C. 552a (d)(1), (2), (3), and (4) of the Privacy Act pursuant to 5 U.S.C. 552a (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e), and have been published in the **Federal Register**.

JUSTICE/CRT-009

SYSTEM NAME:

Civil Rights Division Travel Reports, CRT-009.

SYSTEM LOCATION:

United States Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

All persons who have filed travel authorization forms or travel voucher forms for official travel on behalf of CRT.

CATEGORIES OF RECORDS IN THE SYSTEM:

The Division's filing system contains information concerning travel expenditures which were recorded on travel authorization forms and travel voucher forms by CRT employees or other persons authorized to travel for CRT and submitted to the Budget and Finance Branch of CRT.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The records in this system of records are kept under the authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

PURPOSE(S):

One purpose of this system is to assist employees and officials of the Division to measure and track expenditures within the Division. Other purposes are to assist the Division in preparing reports within various sections to control and review expenditures.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

A record maintained in this system of records may be disseminated as a routine use of such records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or in informal discovery proceedings;

(3) A record may be disseminated to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(5) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(6) A record from a system of records may be disclosed as a routine use to

National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(7) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility; and

(8) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law-criminal, civil or regulatory in nature-the relevant records may be referred to the appropriate Federal, State, local, foreign, or Tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**STORAGE:**

Records are stored in hard copy and electronic form.

RETRIEVABILITY:

Records in this system are retrieved by the names of those individuals identified under the caption "Categories of individuals covered by the system."

SAFEGUARDS:

Information in the system is unclassified. However, the records are protected in accordance with applicable Department security regulations for systems of records. Records are stored in locked cabinets and access to the computer is limited to those personnel who have a need for access to perform their official duties.

RETENTION AND DISPOSAL:

Records are maintained on the system while current and required for official Government use. When no longer needed on an active basis, the records are transferred to computer tape and stored in accordance with Departmental security regulations for systems of records. Final disposition will be in accordance with records retirement or

destruction as scheduled by NARA in General Records Schedule 9.

SYSTEM MANAGER(S) AND ADDRESS:

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

NOTIFICATION PROCEDURE:

Same as the above.

RECORD ACCESS PROCEDURES:

Requests by former employees for access to records in this system may be made in writing with the envelope and letter clearly marked "Privacy Act Request." The request should clearly state the dates on which official travel was taken. The requestor should also provide the full name of the individual involved, his or her current address, date and place of birth, notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), any other known information which may be of assistance in locating the record, and a return address for transmitting the information. Access requests will be directed to the System Manager. Present employees may request access by contacting the System Manager directly.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Sources of information are CRT employees and other authorized persons who file travel authorization and travel voucher forms.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 03-20342 Filed 8-8-03; 8:45 am]

BILLING CODE 4410-13-P

DEPARTMENT OF LABOR**Mine Safety and Health Administration****Proposed Information Collection Request Submitted for Public Comment and Recommendations; Explosive Materials and Blasting Units**

ACTION: Notice.

SUMMARY: The Department of Labor, as part of its continuing effort to reduce

Exhibit 11

determination is negative, upon notice of an affirmative final determination in those investigations under section 735(a) of the Act. Parties that filed entries of appearance in the preliminary phase of the investigations need not enter a separate appearance for the final phase of the investigations. Industrial users, and, if the merchandise under investigation is sold at the retail level, representative consumer organizations have the right to appear as parties in Commission antidumping and countervailing duty investigations. The Secretary will prepare a public service list containing the names and addresses of all persons, or their representatives, who are parties to the investigations.

Background

On May 3, 2005, a petition was filed with the Commission and Commerce by the Diamond Sawblade Manufacturers' Coalition and its individual members: Blackhawk Diamond, Inc., Fullerton, CA; Diamond B, Inc., Santa Fe Springs, CA; Diamond Products, Elyria, OH; Dixie Diamond, Lilburn, GA; Hoffman Diamond, Punxsutawney, PA; Hyde Manufacturing, Southbridge, MA; Sanders Saws, Honey Brook, PA; Terra Diamond, Salt Lake City, UT; and Western Saw, Inc., Oxnard, CA, alleging that an industry in the United States is materially injured and threatened with material injury by reason of LTFV imports of diamond sawblades and parts thereof from China and Korea. Accordingly, effective May 3, 2005, the Commission instituted antidumping duty investigation Nos. 731-TA-1092-1093 (Preliminary).

Notice of the institution of the Commission's investigations and of a public conference to be held in connection therewith was given by posting copies of the notice in the Office of the Secretary, U.S. International Trade Commission, Washington, DC, and by publishing the notice in the *Federal Register* of May 10, 2005 (70 FR 24612) and May 26, 2005 (70 FR 30480). The conference was held in Washington, DC, on June 15, 2005, and all persons who requested the opportunity were permitted to appear in person or by counsel.

The Commission transmitted its determination in these investigations to the Secretary of Commerce on July 18, 2005. The views of the Commission are contained in USITC Publication 3791 (August 2005), entitled *Diamond Sawblades and Parts Thereof from China and Korea: Investigation Nos. 731-TA-1092 and 1093 (Preliminary)*.

Issued: July 25, 2005.

By order of the Commission.
Marilyn R. Abbott,
Secretary to the Commission.
[FR Doc. 05-15023 Filed 7-28-05; 8:45 am]
BILLING CODE 7020-02-P

DEPARTMENT OF JUSTICE

[AAG/A Order No. 004-2005]

Privacy Act of 1974; System of Records

Pursuant to the Privacy Act of 1974 (5 U.S.C. 552a), the Department of Justice, Civil Rights Division (CRT), proposes to modify the following system of records previously modified and published in full text in the *Federal Register* on August 11, 2003 (68 Fed. Reg. 47611): Central Civil Rights Division Index File and Associated Records, JUSTICE/CRT-001.

CRT is adding one new routine use to this system of records. The records in this system of records are maintained by the Civil Rights Division in order to carry out its responsibilities to investigate and enforce federal statutes affecting civil rights. This routine use allows the disclosure of information explaining the Department's decision to close a criminal matter to the local community or public when the incident investigated has become a matter of public knowledge, the investigation is closed, and the Assistant Attorney General, Civil Rights Division, personally determines that, because there is a reasonable potential for civil unrest or a severe loss of confidence by the public in the investigative process, the disclosure of such information is appropriate. The release of information in the new routine use is compatible with the purpose of this system as use of the information is necessary and proper to carry out legitimate government purposes.

In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment on the proposed new routine use disclosure. The Office of Management and Budget (OMB), which has oversight responsibility of the Act, requires a 40-day period in which to conclude its review of the system. Therefore, please submit any comments by August 29, 2005. The public, OMB and the Congress are invited to submit comments to: Mary Cahill, Management and Planning Staff, Justice Management Division, Department of Justice, Room 1400 National Place Building, NW., Washington, DC 20530. If no comments are received, the proposal will be

implemented without further notice in the *Federal Register*.
In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and Congress on the proposed new routine use.

Dated: July 20, 2005.
Paul R. Corts,
Assistant Attorney General for Administration.

JUSTICE/CRT-001

SYSTEM NAME:

Central Civil Rights Division Index File and Associated Records, CRT-001.

* * * * *

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

* * * * *

* * * [Add the new routine use (16) to read as follows.]

(16) To the local community or public when the incident investigated has become a matter of public knowledge, the investigation is closed, and the Assistant Attorney General, Civil Rights Division, personally determines that, because there is a reasonable potential for civil unrest or a severe loss of confidence by the public in the investigative process, the disclosure of information explaining the Department's decision to close a criminal matter is appropriate.

* * * * *

[FR Doc. 05-14944 Filed 7-28-05; 8:45 am]
BILLING CODE 4410-13-P

DEPARTMENT OF LABOR

Employment Standards Administration; Wage and Hour Division

Minimum Wages for Federal and Federally Assisted Construction; General Wage Determination Decisions

General wage determination decisions of the Secretary of Labor are issued in accordance with applicable law and are based on the information obtained by the Department of Labor from its study of local wage conditions and data made available from other sources. They specify the basic hourly wage rates and fringe benefits which are determined to be prevailing for the described classes of laborers and mechanics employed on construction projects of a similar character and in the localities specified therein.

The determinations in these decisions of prevailing rates and fringe benefits have been made in accordance with 29

Exhibit 12

statement of position. See generally GX 4. So too, the Government's Request for Final Agency Action does not address whether Dr. Pasic submitted a written statement.¹ See generally Gov. Request for Final Agency Action.

In her declaration, the DI stated that she had obtained a copy of Dr. Pasic's Registration and Registration History. GX 4, at 3. According to the DI, "Dr. Pasic allowed his . . . registration to lapse on March 31, 2017" and has not "made any request—timely or untimely—to renew his registration." *Id.*

On May 2, 2017, the Government submitted its Request for Final Agency Action. Therein, the Government noted that the case is moot because Dr. Pasic has allowed his registration to expire and has not submitted an application. Request for Final Agency Action, at 3 (citing *Victor B. Williams*, 80 FR 50029 (2015)). However, while the Government recognizes that the matter is moot, it requests that I issue "a final order . . . setting forth the following facts and conclusions of law" related to the suspension of his state authority to "memorialize the outcome of this proceeding for the record and for purpose of evaluating future applications." *Id.*

I grant the Government's request but only with respect to its request that I dismiss this case as moot. Were I to make the factual findings and legal conclusions requested by the Government, I would be issuing an advisory opinion. Though an administrative agency is not subject to the case or controversy requirements of Article III, relevant authority suggests that in the event Respondent sought judicial review of the decision, the federal courts would lack jurisdiction to review that part of the decision. It is settled, however, that where the federal courts lack the power to review an agency decision because of intervening mootness, the court vacates the agency's order. See *A.L. Mechling Barge Lines, Inc. v. United States*, 368 U.S. 324, 329 (1961) (vacating administrative orders which had become unreviewable in federal court); see also *American Family Life Assurance Co. v. FCC*, 129 F.3d 625, 630 (D.C. Cir. 1997) ("Since *Mechling*, we have, as a matter of course, vacated agency orders in cases that have become moot by the time of judicial review."). See also *Samuel H. Albert*, 74 FR 54851, 54852 (2009). As the requested factual findings and legal conclusions would be

subject to vacation on judicial review, there is no point to making them.

Because Respondent's registration has expired and he has not filed an application, whether timely or not, this case is now moot. See *Williams*, 80 FR at 50029; see also *William W. Nucklos*, 73 FR 34330 (2008); *Ronald J. Riegel*, 63 FR 67132, 67133 (1988). Accordingly, I will dismiss the Order to Show Cause.

Order

Pursuant to the authority vested in me by 21 U.S.C. 824(a), as well as 28 CFR 0.100(b), I order that the Order to Show Cause issued to Josip Pasic, M.D., be, and it hereby is, dismissed. This Order is effective immediately.

Dated: May 16, 2017.

Chuck Rosenberg,

Acting Administrator.

[FR Doc. 2017-10742 Filed 5-24-17; 8:45 am]

BILLING CODE 4410-09-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 004-2017]

Privacy Act of 1974; System of Records

AGENCY: United States Department of Justice.

ACTION: Notice of modified Systems of Records; blanket routine use.

SUMMARY: Pursuant to the Privacy Act of 1974, 5 and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the United States Department of Justice (Department or DOJ) proposes to modify the DOJ System of Records Notices for the DOJ systems of records listed below.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is subject to a 30-day notice and comment period. Please submit any comments by June 26, 2017.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments to the U.S. Department of Justice, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, National Place Building, 1331 Pennsylvania Avenue NW., Suite 1000, Washington, DC 20530-0001, by facsimile at 202-307-0693, or email at privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Andrew A. Proia, Attorney Advisor, Office of Privacy and Civil Liberties, National Place Building, 1331 Pennsylvania Avenue NW., Suite 1000, Washington, DC 20530-0001, by

facsimile at 202-307-0693, or email at privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

SUPPLEMENTARY INFORMATION: On May 22, 2007, OMB issued Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, to the heads of all executive departments and agencies. In its memorandum, OMB required agencies to publish a routine use for their systems of records specifically applying to the disclosure of information in connection with response and remedial efforts in the event of a breach of personally identifiable information. DOJ published a notice in the *Federal Register*, 72 FR 3410 (January 25, 2007), modifying all DOJ System of Records Notices by adding a routine use to address the limited disclosure of records related to a suspected or confirmed breach within the Department, consistent with OMB requirements. Since that time, all new DOJ System of Records Notices published by the Department, as well as significantly modified System of Records Notices that were republished in full, included a breach response routine use consistent with the requirements in OMB Memorandum M-07-16.

On January 3, 2017, OMB issued Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, to the heads of all executive departments and agencies. OMB Memorandum M-17-12 rescinds and replaces OMB Memorandum M-07-16 and updates agency routine use requirements for responding to a breach. Specifically, OMB Memorandum M-17-12 requires all Senior Agency Officials for Privacy to ensure that their agency's System of Records Notices include a routine use for the disclosure of information necessary to respond to a breach of the agency's personally identifiable information. Additionally, OMB Memorandum M-17-12 requires agencies to add a routine use to ensure that agencies are able to disclose records in their systems of records that may reasonably be needed by another agency in responding to a breach.

To satisfy the routine use requirements in OMB Memorandum M-17-12, DOJ is issuing two notices in the *Federal Register* to modify all of the Department's System of Records Notices. The records maintained in many DOJ systems of records are still subject to the Department's blanket breach response routine use published

¹ Because I conclude that this matter is now moot, I deem it unnecessary to remand the matter for clarification as to whether Dr. Pasic submitted a written statement.

at 72 FR 3410 (January 25, 2007). For these DOJ systems of records, this notice rescinds 72 FR 3410 (January 25, 2007) and adds the two routine uses required by OMB Memorandum M–17–12.

Other DOJ systems of records have been created or significantly modified since 72 FR 3410 (January 25, 2007) added the previous, OMB-required breach response routine use. The DOJ System of Records Notices for these DOJ systems of records incorporated the OMB Memorandum M–07–16 breach response routine use in their “ROUTINE USES” section, rather than relying on the routine use published at 72 FR 3410 (January 25, 2007). These System of Records Notices are not affected by this notice publication. Elsewhere in the **Federal Register**, the Department is

modifying the DOJ System of Records Notices for the DOJ systems of records that do not rely on the breach response routine use published at 72 FR 3410 (January 25, 2007). The DOJ System of Records Notices for these DOJ systems of records are being modified separately to ensure continuity with their previous notice publications. Pursuant to OMB Memorandum M–17–12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017), this notice: (1) Rescinds the breach response routine use published at 72 FR 3410 (January 25, 2007); (2) revises the breach response routine use for the DOJ systems of records, listed below; and (3) adds a new routine use to the DOJ systems of records, listed below, to

ensure that the Department can assist another agency in responding to a confirmed or suspected breach, as appropriate.

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and to Congress on this notice of modified systems of records.

Dated: May 19, 2017.

Peter A. Winn,

Acting Chief Privacy and Civil Liberties Officer, United States Department of Justice.

United States Department of Justice System of Records Notices and citations follow. An asterisk (*) designates the last full **Federal Register** notice that includes all of the elements that are required to be in a System of Records Notice.

System No. and name	Federal Register, citation(s)
JUSTICE/DOJ–001, Accounting Systems for the Department of Justice	69 FR 31406*, 71 FR 142, 72 FR 3410, 75 FR 13575.
JUSTICE/DOJ–002, DOJ Computer Systems Activity & Access Records	64 FR 73585*, 66 FR 8425, 72 FR 3410.
JUSTICE/DOJ–003, Correspondence Management Systems (CMS) for the Department of Justice	66 FR 29992*, 66 FR 34743, 67 FR 65598, 72 FR 3410.
JUSTICE/DOJ–005, Nationwide Joint Automated Booking System (JABS)	71 FR 52821*, 72 FR 3410.
JUSTICE/DOJ–006, Personnel Investigation and Security Clearance Records for the Department of Justice	67 FR 59864*, 69 FR 65224, 72 FR 3410.
JUSTICE/DOJ–007, Reasonable Accommodations for the Department of Justice	67 FR 34955*, 72 FR 3410.
JUSTICE/DOJ–008, Department of Justice Grievance Records	68 FR 61696*, 69 FR 47179, 72 FR 3410.
JUSTICE/DOJ–009, Emergency Contact Systems for the Department of Justice	69 FR 1762*, 72 FR 3410.
JUSTICE/DOJ–010, Leave Sharing Systems	69 FR 22557*, 69 FR 47179, 72 FR 3410.
JUSTICE/DOJ–011, Access Control System (ACS)	69 FR 70279*, 72 FR 3410.
JUSTICE/DOJ–012, Department of Justice Regional Data Exchange System (RDEX)	70 FR 39790*, 70 FR 72315, 72 FR 3410, 72 FR 4532.
JUSTICE/ASG–001, General Files System of the Office of the Associate Attorney General	69 FR 22872*, 72 FR 3410.
JUSTICE/ATF–001, Administrative Record System	68 FR 3551, 552*, 72 FR 3410.
JUSTICE/ATF–003, Criminal Investigation Report System	68 FR 3551, 553*, 72 FR 3410.
JUSTICE/ATF–006, Internal Security Record System	68 FR 3551, 555*, 72 FR 3410.
JUSTICE/ATF–007, Personnel Record System	68 FR 3551, 556*, 72 FR 3410.
JUSTICE/ATF–008, Regulatory Enforcement Record System	68 FR 3551, 558*, 72 FR 3410.
JUSTICE/ATF–009, Technical and Scientific Services Record System	68 FR 3551, 560*, 72 FR 3410.
JUSTICE/ATF–010, Training and Professional Development Record System	68 FR 3551, 562*, 72 FR 3410.
JUSTICE/ATR–001, Antitrust Division Expert Witness File	54 FR 42060, 061*, 66 FR 8425, 72 FR 3410.
JUSTICE/ATR–003, Index of Defendants in Pending and Terminated Antitrust Cases	60 FR 52690*, 66 FR 8425, 72 FR 3410.
JUSTICE/ATR–004, Statements by Antitrust Division Officials (ATD Speech File)	60 FR 52690, 691*, 66 FR 8425, 72 FR 3410.
JUSTICE/ATR–005, Antitrust Management Information System (AMIS)—Time Reporter	53 FR 40502*, 66 FR 8425, 72 FR 3410.
JUSTICE/ATR–006, Antitrust Management Information System (AMIS)—Monthly Report	63 FR 8659*, 66 FR 8425, 66 FR 17200, 72 FR 3410.
JUSTICE/ATR–007, Antitrust Division Case Cards	60 FR 52690, 692*, 66 FR 8425, 72 FR 3410.
JUSTICE/ATR–009, Public Complaints and Inquiries File	45 FR 75898, 902*, 66 FR 8425, 72 FR 3410.
JUSTICE/ATR–014, Civil Investigative Demand (CID) Tracking System	60 FR 52690, 694*, 66 FR 8425, 72 FR 3410.
JUSTICE/BOP–001, Prison Security and Intelligence Record System	67 FR 41449*, 72 FR 3410.
JUSTICE/BOP–004, Inmate Administrative Remedy Record System	67 FR 57244*, 72 FR 3410.
JUSTICE/BOP–005, Inmate Central Records System	67 FR 31371*, 72 FR 3410, 77 FR 24982, 81 FR 22639.
JUSTICE/BOP–006, Inmate Trust Fund Accounts and Commissary Record System	67 FR 11711*, 72 FR 3410.
JUSTICE/BOP–007, Inmate Physical and Mental Health Record System	67 FR 11712*, 72 FR 3410.
JUSTICE/BOP–008, Inmate Safety and Accident Compensation Record System	67 FR 41452*, 72 FR 3410.
JUSTICE/BOP–009, Administrative Claims Record System	67 FR 41453*, 72 FR 3410.
JUSTICE/BOP–010, Access Control Entry-Exit System	67 FR 16760*, 72 FR 3410.
JUSTICE/BOP–011, Telephone Activity Record System	67 FR 16762*, 71 FR 9606, 72 FR 3410, 76 FR 79216.
JUSTICE/BOP–012, Office of Internal Affairs Investigative Records	67 FR 9321*, 72 FR 3410.
JUSTICE/BOP–013, Inmate Electronic Message Record System	70 FR 69594*, 72 FR 3410, 76 FR 79216.
JUSTICE/BOP–015, Outside Employment Requests Record System	67 FR 16763*, 72 FR 3410.

System No. and name	Federal Register, citation(s)
JUSTICE/BOP-101, The National Institute of Corrections Technical Resource Provider Record System.	65 FR 11342*, 66 FR 8425, 72 FR 3410.
JUSTICE/BOP-103, National Institute of Corrections Academy Record System	64 FR 70286*, 66 FR 8425, 72 FR 3410.
JUSTICE/BOP-104, National Institute of Corrections Mailing List & Information Center Contacts Records System.	64 FR 70287*, 66 FR 8425, 72 FR 3410.
JUSTICE/CIV-001, Civil Division Case File System	63 FR 8659*, 66 FR 8425, 66 FR 17200, 66 FR 36593, 72 FR 3410.
JUSTICE/CIV-002, Civil Division Case File System: Customs Litigation	45 FR 2215, 217*, 66 FR 8425, 72 FR 3410.
JUSTICE/CIV-003, Office of Alien Property File System	42 FR 53288, 324*, 66 FR 8425, 72 FR 3410.
JUSTICE/CIV-004, Swine Flu Administrative Claim File System	43 FR 44708*, 66 FR 8425, 72 FR 3410.
JUSTICE/CIV-005, Annuity Brokers List System	68 FR 17401*, 72 FR 3410.
JUSTICE/CIV-006, Consumer-Inquiry Investigatory System	53 FR 40506*, 66 FR 8425, 72 FR 3410.
JUSTICE/CIV-008, September 11th Victim Compensation Fund of 2001 File System	66 FR 65991*, 66 FR 8425, 72 FR 3410.
JUSTICE/COPS-001, Police Corps System	62 FR 1130, 131*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-002, Criminal Division Witness Security File	52 FR 47188*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-003, File of Names Checked to Determine if those Individuals Have Been the Subject of an Electronic Surveillance.	52 FR 47189*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-006, Information File on Individuals and Commercial Entities Known or Suspected of Being Involved in Fraudulent Activities.	42 FR 53288, 336*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-008, Name Card File on Department of Justice Personnel Authorized to have Access to the Classified Files of the Department of Justice.	52 FR 47193*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-012, Organized Crime and Racketeering Section, General Index File and Associated Records.	55 FR 49146, 147*, 66 FR 8425, 66 FR 17200, 72 FR 3410.
JUSTICE/CRM-014, Organized Crime and Racketeering Section, Intelligence and Special Services Unit, Information Request System.	42 FR 53288, 343*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-019, Requests to the Attorney General for Approval of Applications to Federal Judges for Electronic Interceptions.	52 FR 47198*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-021, The Stocks and Bonds Intelligence Control Card File System	52 FR 47199*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-022, Witness Immunity Records	52 FR 47200*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-025, Tax Disclosure Index File and Associated Records	52 FR 47202*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRM-026, International Prisoner Transfer Case Files-International Prisoner Transfer Tracking System.	68 FR 22739*, 72 FR 3410.
JUSTICE/CRM-027, Office of Special Investigation (OSI) Displaced Persons Listings	52 FR 47204*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRS-001, Operational Data Information System	45 FR 2215, 220*, 66 FR 8425, 72 FR 3410.
JUSTICE/CRT-001, Central Civil Rights Division Index File and Associated Records	68 FR 47610, 611*, 70 FR 43904, 72 FR 3410.
JUSTICE/CRT-003, Civil Rights Interactive Case Management System	68 FR 47610, 613*, 72 FR 3410.
JUSTICE/CRT-004, Registry of Names of Interested Persons Desiring Notification of Submissions Under Section 5 of the Voting Rights Act.	68 FR 47610, 614*, 72 FR 3410.
JUSTICE/CRT-007, Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission.	68 FR 47610, 615*, 72 FR 3410.
JUSTICE/CRT-009, Civil Rights Division Travel Reports	68 FR 47610, 616*, 72 FR 3410.
JUSTICE/DAG-006, Presidential Appointee Candidate Records System	50 FR 42607*, 66 FR 8425, 72 FR 3410.
JUSTICE/DAG-007, Presidential Appointee Records System	50 FR 42608*, 66 FR 8425, 72 FR 3410.
JUSTICE/DAG-008, Special Candidates for Presidential Appointments and Noncareer SES Positions Records System.	59 FR 45005*, 66 FR 8425, 72 FR 3410.
JUSTICE/DAG-010, United States Judge and Department of Justice Presidential Appointee Records.	50 FR 42612*, 66 FR 8425, 72 FR 3410.
JUSTICE/DAG-013, General Files System	57 FR 8474*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-001, Air Intelligence Program	52 FR 472182, 06*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-INS-111, Automated Intelligence Records System (Pathfinder)	55 FR 49146, 182*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-002, Clandestine Laboratory Seizure System (CLSS)	68 FR 3894*, 72 FR 3410.
JUSTICE/DEA-003, Automated Records and Consolidated Orders System—Diversion Analysis and Detection System (ARCOS-DADS).	69 FR 51104*, 72 FR 3410.
JUSTICE/DEA-005, Controlled Substances Act Registration Records (CSA)	52 FR 47182, 208*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-010, Planning and Inspection Division Records	52 FR 47182, 213*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-011, Operations Files	52 FR 47182, 214*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-012, Registration Status-Investigation Records	52 FR 47182, 215*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-013, Security Files	52 FR 47182, 215*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-015, Training Files	52 FR 47182, 217*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-017, Grants of Confidentiality Files (GCF)	52 FR 47182, 218*, 66 FR 8425, 72 FR 3410.

24150

Federal Register / Vol. 82, No. 100 / Thursday, May 25, 2017 / Notices

System No. and name	Federal Register, citation(s)
JUSTICE/DEA-020, Essential Chemical Reporting System	52 FR 47219*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-021, DEA Aviation Unit Reporting System	65 FR 24986, 987*, 66 FR 8425, 72 FR 3410.
JUSTICE/DEA-022, El Paso Intelligence Center (EPIC) Seizure System (ESS)	71 FR 36362*, 72 FR 3410.
JUSTICE/ENRD-003, Environment & Natural Resources Division Case & Related Files System ...	65 FR 8990*, 66 FR 8425, 70 FR 61159, 72 FR 3410.
JUSTICE/EOIR-001, Records and Management Information System	69 FR 26179*, 72 FR 3410
JUSTICE/EOIR-003, Practitioner Complaint—Disciplinary Files	64 FR 49237*, 66 FR 8425, 72 FR 3410.
JUSTICE/BIA-001, Decisions of the Board of Immigration Appeals	48 FR 5331*, 66 FR 8425, 72 FR 3410.
JUSTICE/BIA-002, Roster of Organizations and their Accredited Representatives Recognized by the Board of Immigration Appeals.	45 FR 75908*, 66 FR 8425, 72 FR 3410.
JUSTICE/FBI-001, National Crime Information Center (NCIC)	64 FR 52343*, 66 FR 8425, 72 FR 3410.
JUSTICE/FBI-002, The FBI Central Records System	63 FR 8659, 671*, 66 FR 8425, 66 FR 17200, 72 FR 3410.
JUSTICE/FBI-003, Bureau Mailing Lists	70 FR 7513*, 72 FR 3410.
JUSTICE/FBI-006, Electronic Surveillance (ELSUR) Indices	70 FR 7513, 514*, 72 FR 3410.
JUSTICE/FBI-008, Bureau Personnel Management System	58 FR 51875*, 66 FR 8425, 72 FR 3410.
JUSTICE/FBI-010, Employee Travel Vouchers and Individual Earning Records	52 FR 47248*, 66 FR 8425, 72 FR 3410.
JUSTICE/FBI-011, Employee Health Records	58 FR 51875*, 66 FR 8425, 72 FR 3410.
JUSTICE/FBI-013, Security Access Control System (SACS)	70 FR 7513, 516*, 72 FR 3410.
JUSTICE/FBI-015, National Center for the Analysis of Violent Crime (NCAVC)	58 FR 51877*, 66 FR 8425, 72 FR 3410.
JUSTICE/FBI-016, FBI Counterdrug Information Indices System (CIIS)	59 FR 29824*, 66 FR 8425, 72 FR 3410.
JUSTICE/FBI-017, National DNA Index System (NDIS)	61 FR 37495*, 66 FR 8425, 72 FR 3410.
JUSTICE/FBI-018, National Instant Criminal Background Check System (NICS)	63 FR 65223*, 65 FR 78190, 66 FR 6676, 66 FR 8425, 66 FR 12959, 72 FR 3410.
JUSTICE/FBI-BRU, Blanket Routine Uses (BRU) Applicable to More Than One FBI Privacy Act System of Records.	66 FR 33558*, 70 FR 7513, 517, 72 FR 3410.
JUSTICE/FTTTF-001, Flight Training Candidates File System	67 FR 39839*, 67 FR 47570, 72 FR 3410.
JUSTICE/JMD-002, Controlled Substances Act Nonpublic Records	66 FR 38000*, 72 FR 3410
JUSTICE/JMD-017, Department of Justice Employee Transportation Facilitation System	66 FR 20683*, 72 FR 3410, 72 FR 54460.
JUSTICE/JMD-022, Department of Justice Consolidated Asset Tracking System (CATS)	71 FR 29170*, 72 FR 3410.
JUSTICE/JMD-023, Federal Bureau of Investigation Whistleblower Case Files	70 FR 53253*, 72 FR 3410, 72 FR 15906, 72 FR 30631.
JUSTICE/JMD-024, Attorney Student Loan Repayment Program Applicant Files	71 FR 64740*, 72 FR 3410.
JUSTICE/NDIC-001, National Drug Intelligence Center Data Base	58 FR 21995*, 66 FR 8425, 72 FR 3410.
JUSTICE/OAG-001, General Files System	50 FR 37294*, 66 FR 8425, 72 FR 3410.
JUSTICE/OIG-004, OIG Employee Training Records	64 FR 68375*, 66 FR 8425, 72 FR 3410.
JUSTICE/OIG-005, OIG Firearms Qualifications System	64 FR 68376*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-001, Equipment Inventory	58 FR 51879*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-004, Grants Management Information System	53 FR 40526*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-006, Congressional and Public Affairs System	52 FR 47276*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-007, Public Information System	45 FR 75936*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-008, Civil Rights Investigative System	53 FR 40528*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-009, Federal Advisory Committee Membership Files	53 FR 40529*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-010, Technical Assistance Resource Files	53 FR 40530*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-011, Registered Users File—National Criminal Justice Reference Service (NCJRS)	58 FR 51879*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-012, Public Safety Officers Benefits System	64 FR 25070*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-013, Denial of Federal Benefits Clearinghouse System (DEBAR)	64 FR 25071*, 66 FR 8425, 72 FR 3410.
JUSTICE/OJP-014, Victims of International Terrorism Expense Reimbursement Program	71 FR 44709*, 72 FR 3410.
JUSTICE/OLP-002, United States Judges Records System.	50 FR 30309*, 66 FR 8425, 72 FR 3410.
JUSTICE/OLP-003, General Files System of the Office of Legal Policy	50 FR 37299*, 66 FR 8425, 72 FR 3410.
JUSTICE/OSCW-001, Caselink Document Database for Office of Special Counsel—Waco	65 FR 53749*, 66 FR 8425, 72 FR 3410.
JUSTICE/PAO-001, News Release, Document and Index System	42 FR 53288, 364*, 66 FR 8425, 72 FR 3410.
JUSTICE/PRC-001, Docket, Scheduling and Control	52 FR 47182, 281*, 66 FR 8425, 72 FR 3410.
JUSTICE/PRC-003, Inmate and Supervision Files	53 FR 7813*, 66 FR 8425, 72 FR 3410.
JUSTICE/PRC-004, Labor and Pension Case, Legal File and General Correspondence System ...	53 FR 40533*, 66 FR 8425, 72 FR 3410.
JUSTICE/PRC-005, Office Operation and Personnel System	53 FR 40535*, 66 FR 8425, 72 FR 3410.
JUSTICE/PRC-006, Statistical, Educational and Developmental System	52 FR 47182, 287*, 66 FR 8425, 72 FR 3410.
JUSTICE/PRC-007, Workload Record, Decision Result, and Annual Report System	53 FR 40535*, 66 FR 8425, 72 FR 3410.
JUSTICE/TAX-001, Criminal Tax Case Files, Special Project Files, Docket Cards, and Associated Records.	71 FR 11446, 447*, 72 FR 3410.
JUSTICE/TAX-002, Tax Division Civil Tax Case Files, Docket Cards, and Associated Records	71 FR 11446, 449*, 72 FR 3410.
JUSTICE/TAX-003, Files of Applications for Attorney and Non-Attorney Positions with the Tax Division.	71 FR 11446, 451*, 72 FR 3410.
JUSTICE/USA-001, Administrative File	48 FR 56662*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-002, A.U.S.A. Applicant Files	48 FR 38329*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-003, Citizen Complaint Files	54 FR 42088*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-005, Civil Case Files	53 FR 1864*, 63 FR 8659, 66 FR 8425, 66 FR 17200, 72 FR 3410.
JUSTICE/USA-006, Consumer Complaints	54 FR 42090*, 66 FR 8425, 72 FR 3410.

System No. and name	Federal Register, citation(s)
JUSTICE/USA-007, Criminal Case Files	53 FR 1864*, 63 FR 8659, 64 FR 71499, 66 FR 8425, 66 FR 17200, 72 FR 3410.
JUSTICE/USA-009, Kline District of Columbia and Maryland Stock and Land Fraud Interrelationship Filing System.	54 FR 42092*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-010, Major Crimes Division Investigative Files	54 FR 42094*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-011, Prosecutor's Management Information System (PROMIS)	54 FR 42095*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-012, Security Clearance Forms for Grand Jury Reporters	48 FR 5386*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-013, U.S. Attorney, District of Columbia Superior Court Division, Criminal Files	54 FR 42097*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-014, Pre-Trial Diversion Program Files	48 FR 38344*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-016, Assistant United States Attorney Applicant Records System	57 FR 8487*, 66 FR 8425, 72 FR 3410.
JUSTICE/USA-017, Appointed Assistant United States Attorneys Personnel System	57 FR 8488*, 66 FR 8425, 72 FR 3410.
JUSTICE/USM-019, Merit Promotion Open Season Records System (MPOS)	71 FR 29668*, 72 FR 3410.
JUSTICE/UST-001, Bankruptcy Case Files and Associated Records	71 FR 59818, 819*, 72 FR 3410.
JUSTICE/UST-002, Bankruptcy Trustee Oversight Records	71 FR 59818, 822*, 72 FR 3410.
JUSTICE/UST-003, U.S. Trustee Program Timekeeping Records	71 FR 59818, 824*, 72 FR 3410.
JUSTICE/UST-004, U.S. Trustee Program Case Referral System	71 FR 59818, 825*, 72 FR 3410.
JUSTICE/UST-005, Credit Counseling and Debtor Education Files and Associated Records	71 FR 59818, 827*, 72 FR 3410.

The routine use published at 72 FR 3410 (January 25, 2007) is hereby rescinded for the DOJ System of Records Notices, listed above, and replaced as follows:

* * * * *

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

* * * * *

[FR Doc. 2017-10780 Filed 5-24-17; 8:45 am]

BILLING CODE 4410-NW-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 005-2017]

Privacy Act of 1974; System of Records

AGENCY: United States Department of Justice.

ACTION: Notice of modified Systems of Records.

SUMMARY: Pursuant to the Privacy Act of 1974, and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the United States Department of Justice (Department or DOJ) proposes to modify the DOJ System of Records Notices for the DOJ systems of records listed below.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is subject to a 30-day notice and comment period. Please submit any comments by June 26, 2017.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments to the U.S. Department of Justice, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, National Place Building, 1331 Pennsylvania Avenue NW., Suite 1000, Washington, DC 20530-0001, by facsimile at 202-307-0693, or email at privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Andrew A. Proia, Attorney Advisor, Office of Privacy and Civil Liberties, National Place Building, 1331 Pennsylvania Avenue NW., Suite 1000, Washington, DC 20530-0001, by facsimile at 202-307-0693, or email at privacy.compliance@usdoj.gov. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

SUPPLEMENTARY INFORMATION: On May 22, 2007, OMB issued Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, to the heads of all executive departments and agencies. In its memorandum, OMB required agencies to publish a routine use for their systems of records specifically addressing the disclosure of records in connection with the response to, and remedial efforts in the event of, a breach of personally identifiable information. DOJ published a notice in the **Federal Register**, 72 FR 3410 (January 25, 2007), modifying all DOJ System of Records Notices by adding a routine use to address the limited disclosure of records related to a suspected or confirmed breach within the Department, consistent with OMB requirements. Since that time, all new DOJ System of Records Notices published by the Department, as well as significantly modified System of Records Notices that were republished in full, included a breach response routine use consistent with the requirements in OMB Memorandum M-07-16.

On January 3, 2017, OMB issued Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, to the heads of all executive departments and agencies. OMB Memorandum M-17-12 rescinds and replaces OMB Memorandum M-07-16 and updates agency routine use requirements for responding to a breach. Specifically, OMB Memorandum M-17-12 requires all Senior Agency Officials for Privacy to ensure that their agency's System of Records Notices include a routine use for the disclosure of information necessary to respond to a breach of the agency's personally identifiable information. Additionally, OMB Memorandum M-17-12 requires agencies to add a routine use to ensure

Exhibit 13



Privacy Impact Assessment

for the

Systematic Alien Verification for Entitlements “SAVE” Program

DHS Reference No. DHS/USCIS/PIA-006(d)

October 31, 2025



Homeland Security



Abstract

1. The abstract is the single paragraph that will be used to describe the program and the Privacy Impact Assessment.¹

The U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, Verification Division administers the Systematic Alien Verification for Entitlements (SAVE) Program. The SAVE Program is an online inter-governmental service designed to help federal, state, territorial, tribal, local government agencies, benefit-granting agencies, other authorized entities and licensing bureaus, as authorized by law, determine citizenship and immigration status of individuals within their jurisdiction for the purpose of granting benefits, licenses, as well as for other lawful purposes. U.S. Citizenship and Immigration Services is publishing an update to this Privacy Impact Assessment to describe the collection, use, maintenance, and disclosure of personally identifiable information, as well as the risks associated with these updates. The purpose of this update is to discuss the changes to the tool, including: (1) documenting use of the tool for voter registration and voter maintenance list verification, (2) collection of Social Security numbers which may include those of U.S. born citizens for all benefit or license related uses of the program, (3) sharing of information between U.S. Citizenship and Immigration Services, the Social Security Administration, and the Department of State, (4) a new bulk upload feature for the program, and (5) reducing the fee for non-Federal government agencies.

Overview

2. The overview provides the context and background necessary to understand the project's purpose and mission and the justification for operating a privacy sensitive project.

The U.S. Citizenship and Immigration Services administers the SAVE Program. The SAVE Program is an online fee-based intergovernmental initiative designed to help federal, state, tribal, and local government agencies and licensing bureaus confirm immigration status information.²

¹ Pursuant to Section 208 of the E-Government Act of 2002, agencies are required to conduct a Privacy Impact Assessment before developing or procuring Information Technology systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public. The Office of Management and Budget issued Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, which defines "information in identifiable form" as information in an Information Technology system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements. Furthermore, an individual is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence."

² It is the intent of the current Administration to provide more of a supporting role to state, local, tribal, and territory governments. The U.S. Department of Homeland Security has determined to better serve and support non-Federal



Homeland Security

The SAVE Program provides status verifications to requesting federal, state, territorial, tribal, and local government agencies; benefit granting agencies; and other authorized entities and licensing bureaus. The U.S. Citizenship and Immigration Services (or a contractor acting on its behalf) will confirm immigration and/or United States citizenship status as authorized by law, to the extent that such disclosure is necessary to enable these agencies to make decisions. These decisions may relate to: (1) determining eligibility for a federal, state, or local public benefit; (2) issuing a license or grant; (3) issuing a government credential; (4) conducting a background investigation; (5) registering voters or developing/ managing voter maintenance lists; or (6) any other lawful purpose.

A federal, state, territorial, tribal, or local government agency that provides a public benefit or license, or that is otherwise authorized by law to engage in an activity related to the verification of immigration status, may enroll in the SAVE Program as a registered agency. By using the SAVE Program, federal, state, territorial, tribal, and local registered agencies can request immigration status information to determine the applicant's eligibility for a benefit or a license. It is important to note that the program does not make the determinations on an applicant's eligibility for a specific benefit or license or eligibility to vote (at the local, state, or national level). Instead, it provides immigration status information to agencies to allow them to make an informed decision prior to issuing benefits or licenses or denying voting benefits. The registered agency analyzes the SAVE Program's response against the agency's own eligibility criteria to make an award determination. The SAVE Program may not always know the outcome of the benefit adjudication.

The SAVE Program has access to multiple immigration record systems from government agencies to confirm immigration status. All SAVE Program-registered agencies must adhere to a Memorandum of Agreement or Computer Matching Agreement, which include binding responsibilities regarding proper information usage and handling. The Memorandum of Agreement also stipulates the terms for billing and payment, if applicable. As part of its billing and registration process, the SAVE Program collects personally identifiable information, such as the registered agency's point of contact name and professional contact information, as well as registered agency and demographic information. The SAVE Program staff may also collect sensitive information such as registered agency credit card information and other data relevant to the billing process from the federal, state, territorial, tribal, or local government agencies using the SAVE Program. The U.S. Citizenship and Immigration Service collects, maintains, and safeguards this information in accordance with U.S. Department of Homeland Security privacy and information technology policies.

The U.S. Citizenship and Immigration Services is currently implementing a comprehensive

government agencies, by eliminating the fees for their use of the SAVE Program.



optimization of the SAVE Program. The U.S. Citizenship and Immigration Services has developed a phased approach to further the U.S. Department of Homeland Security mission. This Privacy Impact Assessment supports use of the SAVE Program for (1) voter registration and voter maintenance list verification; (2) collection of Social Security numbers, which may include those of U.S. born citizens for all benefit- or license-related uses of the program; (3) sharing of information between U.S. Citizenship and Immigration Services, the Social Security Administration, and the Department of State; (4) a new bulk upload feature for the program; and (5) removing the fee for non-Federal government agencies.

Social Security Administration Data Sharing

On January 20, 2025, and March 25, 2025, the President issued Executive Orders 14159, *Protecting the American People Against Invasion* and 14248, *Preserving and Protecting the Integrity of American Elections* respectively.³ Executive Order 14159 includes a requirement for the Secretary to "...promptly issue guidance to ensure maximum compliance by [Department of Homeland Security] personnel with the provisions of 8 U.S.C. 1373 and 8 U.S.C. 1644 and ensure that State and local governments are provided with the information necessary to fulfill law enforcement, citizenship, or immigration status verification requirements authorized by law...."⁴ Executive Order 14248 outlines that, "...Federal laws, such as the National Voter Registration Act (Pub. L. 103-31) and the Help America Vote Act (Pub. L. 107-252), require States to maintain an accurate and current Statewide list of every legally registered voter in the State. And [Department of Homeland Security] is required to share database information with States upon request so they can fulfill this duty."⁵ Executive Order 14248 directs the Secretary to "...ensure that State and local officials have, without the requirement of the payment of a fee, access to appropriate systems for verifying the citizenship or immigration status of individuals registering to vote or who are already registered..." The Department of Homeland Security is also required under Executive Order 14248, in coordination with the Department of Government Efficiency Administrator, to "review each State's publicly available voter registration list and available records concerning voter list maintenance activities as required by 52 U.S.C. § 20507, alongside Federal immigration databases and State records requested, including through subpoena where necessary and authorized by law, for consistency with Federal requirements."

The Commissioner of Social Security also must assist states in determining whether individuals are eligible to register and vote by taking all appropriate action to make available the Social

³ See *Protecting the American People Against Invasion* (January 2025) available at <https://www.federalregister.gov/documents/2025/03/28/2025-05523/preserving-and-protecting-the-integrity-of-american-elections>; and *Preserving and Protecting the Integrity of American Elections* (March 2025) available at <https://www.federalregister.gov/documents/2025/01/29/2025-02006/protecting-the-american-people-against-invasion>.

⁴ 8 U.S.C. § 1373; 8 U.S.C. § 1644.

⁵ 8 U.S.C. 1373(c).



Homeland Security

Security Number Verification Service, the Death Master File, and any other Federal databases containing relevant information to all State and local election officials engaged in verifying the eligibility of individuals registering to vote or who are already registered.⁶

Most registered agencies may not have access in their voter, benefits, or licenses records to a U.S. Department of Homeland Security-issued identifier, (such as Alien Registration Number (Alien Number or A-number), Naturalization Certificate number, or Citizenship Certificate number) to initiate the initial SAVE Program query. To address this concern, the U.S. Citizenship and Immigration Services is incorporating a feature to allow SAVE Program-registered agencies to query records by Social Security numbers. Registered agencies will provide the U.S. Citizenship and Immigration Services with the individual's first and last name(s), date of birth and a full 9-digit or partial Social Security number. Registered agencies may additionally provide a U.S. Department of Homeland Security enumerator. The U.S. Citizenship and Immigration Services will provide the Social Security Administration with this information and in turn they will provide the U. S. Citizenship and Immigration Service with the following responses:

- Social Security number match (True/False);
- Name match (True/False);
- Date of birth match (True/False);
- Citizenship Indicator;
 - "A" - U.S. citizen;
 - "B" - Legal alien, eligible to work;
 - "C" - Legal alien, not eligible to work;
 - "D" – Other;
 - "E" - Alien student - restricted work authorized; and
 - "F" - Conditionally legalized alien.
- Foreign Born indicator (Citizenship code is not present, but individual was foreign born);
- State/Country code;
- American Samoa indicator (True/False);
- Alien Registration number (where applicable);

⁶ Executive Order 14248 § 3(a).



- Death indicator (Yes / No); and
- Error code descriptions (transaction and record levels).

Of note, if a registered agency provides the names, dates of birth, and Social Security numbers of U.S. citizens by birth, the SAVE Program will maintain and process this information. For instance, a state may provide the U.S. Citizenship and Immigration Services information for all residents that are registered to vote within their jurisdiction. This would include U.S. citizens by birth. The U. S. Citizenship and Immigration Services will process this information as stated above and provide the appropriate response.

The SAVE Program now has a list processor feature to allow registered agencies to upload a list of individuals' case data instead of creating individual cases. A requesting agency, once signed into the program, will have an option to "upload" a list of individuals for the U.S. Citizenship and Immigration Services to verify citizenship and immigration status. Once uploaded, the SAVE Program creates individual cases for everyone identified on the uploaded list. The U. S. Citizenship and Immigration Services then sends from the list to the Social Security Administration the name, Social Security number, and date of birth of the individuals identified by the registered agency. The Social Security Administration then sends the status information (citizenship indicator noted above) back to the SAVE Program. The SAVE Program, if required, also queries other various systems (see below *List of Federal Systems Used to Respond to Registered Agency Queries*), and provides a consolidated result in each case file. The registered agency has the option of logging back into the program after twenty-four hours and searching for each case or generating a Web Agency Audit Report within the SAVE Program that can provide status information for multiple cases.

Additionally, program users will be able to download a list of individuals from the original list that the registered agency submitted, that the U.S. Citizenship and Immigration Services was not able to process. For example, a registered agency's list may not have a unique identifier for several individuals. To capture these incomplete cases, the program creates a spreadsheet that includes everyone who is not processed and requests additional information such as a Social Security number (corrected Social Security number), or Alien Registration Number. The registered agency can then update the spreadsheet provided with the additional information and upload it again into the program. The U.S. Citizenship and Immigration Services then provides the registered agency's account with the following information:

- Verification number (SAVE Program generated);
- Initial request date;
- Identification type;



- Identification number;
- Last name;
- Benefit code;
- Benefit description;
- Initial request response (Lawful status, No lawful status, Deceased);
- Additional request date;
- Additional request response (Lawful status, No lawful status, Deceased);
- Third step request date;
- Third step resolution (Lawful status, No lawful status, Deceased); and
- Closed date.

Department of State Data Sharing

Registered agencies may provide either a U.S. passport number or a photocopy of a U.S. passport as documentation of citizenship or immigration status. If a U.S. passport number is submitted, the SAVE Program will verify it against information from U.S. Department of State-issued passport. Additionally, the SAVE Program will receive or access information in the U.S. Department of State's Consular Consolidated Database / American Citizen Record Query system, which is a consular search engine used by the U.S. Department of State to manage and access records related to United States citizens, particularly for consular protection and services, including managing passport requests and applications.

State Driver's Licensing Agencies and Other Organizations Maintaining Driver's License Information Data Sharing

Within the U.S., driver's licenses are the most widely used form of identification. The SAVE Program can use driver's license and state identification card numbers to check and confirm identity information by working with state driver's licensing agencies and national agencies that store driver's license information for legal purposes (such as the National Law Enforcement Telecommunications System). When the registered agency provides a driver's license or state identification card number as the enumerator to verify the identity of the applicant, the SAVE Program will use state driver's licensing agencies or another source (such as the National Law Enforcement Telecommunications System) to validate the information and gain access to other government enumerators. This will allow the SAVE Program to match against other sources to verify immigration status and U.S. citizenship, which will improve accuracy and efficiency for SAVE registered agencies.



Auditing of Federal and State Oversight Programs Data Sharing

The SAVE Program will support organizations that have entered into required agreements with the U.S. Citizenship and Immigration Services and have a legal oversight authority over a program or benefit type supported by the SAVE Program through reporting capabilities for auditing purposes. User agencies with a legal authority to monitor and audit benefits granted may view case data such as biographic data, enumerators, case submission date/time, and the SAVE Program response information. Reporting options exist for individual agencies and their case data. Additionally, user agencies with legal authority may now be granted SAVE Program access to view other user agencies' case data through a linking mechanism based on either benefit type granted (e.g. Medicare) or by state. This new account type will have reporting options to view case data. Other account types enable user agencies to create cases within the SAVE Program to verify applicant current eligibility for benefits previously granted. This will allow federal and state oversight agencies to ensure user agencies are properly verifying immigration status or citizenship before making an eligibility determination. Oversight agencies can also ensure previously approved applicants remain eligible for the benefits they are receiving.

List of Federal Systems Used to Respond to Registered Agency Queries

The following is a list of federal information systems that the SAVE Program queries for responses to registered agencies:

United States Citizenship and Immigration Services Systems:

- Central Index System;⁷
- Electronic Immigration System;⁸
- Computer Linked Application Information Management System 3;⁹
- Enterprise Citizenship and Immigration Services Centralized Operational Repository;¹⁰
- GLOBAL (not an acronym);

⁷ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CENTRAL INDEX SYSTEM, DHS/USCIS/PIA-009, *available at* [Privacy Documents for USCIS | Homeland Security](#).

⁸ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE USCIS ELECTRONIC IMMIGRATION SYSTEM, DHS/USCIS/PIA-056, *available at* [Privacy Documents for USCIS | Homeland Security](#).

⁹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016, *available at* [Privacy Documents for USCIS | Homeland Security](#).

¹⁰ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE CITIZENSHIP AND IMMIGRATIONS SERVICES CENTRALIZED OPERATIONAL REPOSITORY, DHS/USCIS/PIA-023, *available at* [Privacy Documents for USCIS | Homeland Security](#).



- RAILS (not an acronym);¹¹
- Customer Profile Management System;¹² and
- Salesforce Customer Relationship Management Customer Relationship Management.

Other U.S. Department of Homeland Security Systems:

- U.S. Department of Homeland Security OneNet;
- U.S. Immigration and Customs Enforcement Student and Exchange Visitor Program;¹³
- U.S. Immigration and Customs Enforcement, Enforcement Integrated Database;¹⁴
- U.S. Customs and Border Protection Arrival and Departure Information System;¹⁵ and
- Transportation Security Administration Office of Intelligence and Analysis Technology Infrastructure Modernization Program.¹⁶

Other Federal Agency Systems:

- U.S. Military Entrance Processing Command Integrated Resource System;
- U.S. Department of Education Federal Student Aid Central Processing System;
- U.S. Department of Health and Human Services Centers for Medicare & Medicaid Services;
- U.S. Social Security Administration Numident system;
- U.S. Department of Justice Executive Office for Immigration's Immigration Review Information Exchange System;

¹¹ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR RAILS, DHS/USCIS/PIA-075, *available at* [Privacy Documents for USCIS | Homeland Security](#).

¹² See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE CUSTOMER PROFILE MANAGEMENT SERVICE, DHS/USCIS/PIA-060, *available at* [Privacy Documents for USCIS | Homeland Security](#).

¹³ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT AND EXCHANGE VISITOR PROGRAM, DHS/ICE/PIA-001, *available at* [Privacy Documents for ICE | Homeland Security](#).

¹⁴ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE, DHS/ICE/PIA-015, *available at* [Privacy Documents for ICE | Homeland Security](#).

¹⁵ See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM, DHS/CBP/PIA-024, *available at* [Privacy Documents for CBP | Homeland Security](#).

¹⁶ See U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE TRANSPORTATION SECURITY ADMINISTRATION OFFICE OF INTELLIGENCE AND ANALYSIS TECHNOLOGY INFRASTRUCTURE MODERNIZATION PROGRAM, DHS/TSA/PIA-042, *available at* [Privacy Documents for TSA | Homeland Security](#).



- U.S. Department of State Consular Consolidated Database; and
- U.S. Department of State American Citizen Record Query System.

Fair Information Practice Principles

The U.S. Department of Homeland Security conducts Privacy Impact Assessments on developed or procured information technology systems involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form, as required by Public Law 107-347, Section 208, “The E-Government Act of 2002,” and any applicable and implementing Office of Management and Budget guidance; or proposed rulemakings affecting personal information as required by Section 222(a)(4) of the Homeland Security Act of 2002; or technologies that sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information pursuant to 6 U.S.C § 142(a)(1).

In response to these obligations, the U.S. Department of Homeland Security Privacy Office developed a set of Fair Information Practice Principles¹⁷ from the underlying concepts of the Privacy Act of 1974¹⁸ to encompass the full scope of the information and interactions of the U.S. Department of Homeland Security. The Fair Information Practice Principles account for the nature and purpose of the information being collected in relation to the U.S. Department of Homeland Security’s mission to preserve, protect, and secure. The Fair Information Practice Principles are a set of eight principles that are rooted in the tenets of the Privacy Act.

3. What specific legal authorities and/or agreements permit the collection of information by the project in question?

In accordance with a 1986 Congress mandate, the U.S. Citizenship and Immigration Services, previously the Immigration and Naturalization Service, established the SAVE Program to verify the citizenship and immigration status of individuals seeking government benefits for use by benefit granting agencies when making benefit determinations. The following provides authority for the program to collect, maintain, and share personally identifiable information:

- Immigration and Nationality Act, Public Law 82-414, 66 Statutory 163 (June 27, 1952);
- Homeland Security Act of 2002, Public Law Number 107-296, 116 Statutory 2135

¹⁷ U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (2008), *available at* <https://www.dhs.gov/privacy-policy-guidance>.

¹⁸ Privacy Act of 1974, 5 U.S.C. § 552a, as amended.



(November 25, 2002);

- Immigration Reform and Control Act of 1986, Public Law 99-603, 11 Statutory 3359 (November 6, 1986);
- Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Public Law 104-193, 110 Statutory 2105 (August 22, 1996);
- Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208, 110 Statutory 3009 (September 30, 1996);
- Real ID Act of 2005, Public Law 109-13, 119 Statutory 231 (May 11, 2005);
- Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, 124 Statutory 119 (Mar. 23, 2010), as amended by the Health Care and Education Reconciliation Act of 2010, Public Law 111-152, 124 Stat. 1029 (March 30, 2010);
- Federal Aviation Administration Extension, Safety and Security Act of 2016, Public Law 114-190, 130 Statutory 615 (July 15, 2016); and
- Social Security Act of 1935, Public Law 74-271, 49 Statutory 620 (Aug. 14, 1935) as amended, 42 U.S.C. § 1306.

In addition, the Systematic Alien Verification for Entitlements Program has an obligation under 8 U.S.C. 1373(c) to “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.”

The Social Security Administration is aiding by sending to, and receiving, U.S. Department of Homeland Security and U.S. Citizenship and Immigration Services information regarding the citizenship or immigration status, lawful or unlawful, of individuals within its records. The Social Security Administration is authorized to participate in this information sharing under the authority of the Social Security Act, 42 U.S.C. § 1306, and pursuant to 8 U.S.C. § 1373(a).

4. Will this information be maintained as part of system of records,¹⁹ as defined in the Privacy Act, 5 U.S.C. §552a?

¹⁹ The term “system of records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.



Yes, information retrieved by the Social Security Administration, U.S. Department of State, and registered agencies will be maintained in the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program System of Records.²⁰

5. From which population does the project collect, maintain, use, and/or disseminate personally identifiable information?²¹

- a. Members of the public
- b. U.S. Department of Homeland Security employees and/or contractors
- c. Other federal employees

6. What personally identifiable information is collected, maintained, used, or disseminated?

The U.S. Citizenship and Immigration Services may collect the following information about aliens; legal permanent residents; and U.S. born, naturalized, and derived citizens from registered agencies:

- Name (last, first, middle);
- Unique identifiers;
 - Alien Registration Number (Alien number or A-Number)/U. S. Citizenship and Immigration Services Number;
 - I-94 Arrival/Departure Record number;
 - Student and Exchange Visitor Information System Identification number;
 - Receipt number/card number;
 - Naturalized Certificate number; and
 - Citizenship Certificate number.

²⁰ See DHS/USCIS-004 Systematic Alien Verification for Entitlements, 90 Fed. Reg. 48948 (October 31, 2025), available at [System of Records Notices | Homeland Security](#).

²¹ Personally identifiable information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. See [OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information](#).



- Visa or Passport (Foreign and/or United States) numbers;
- Social Security number or Individual Tax Identification Number;
- Driver's license or state identification number;
- Date of birth;
- Country of birth;
- Citizenship or nationality;
- Class of Admission code and Date of entry;
- File Control Office;
- Benefit sought; and
- Immigration documentation.

The United States Citizenship and Immigration Services shares the following information to the Social Security Administration about U.S. born, naturalized, and/or derived citizens:

- Name (last, first, middle);
- Date of birth;
- Social Security number (full and partial); and
- U.S. Department of Homeland Security-issued identifier (such as Alien Registration Number).

The U. S. Citizenship and Immigration Services maintains the following information from the Social Security Administration:

- Social Security number match (True/False);
- Name match (True/False);
- Date of birth match (True/False);
- Citizenship indicator;
 - "A" - U.S. citizen;
 - "B" - Legal alien, eligible to work;
 - "C" - Legal alien, not eligible to work;
 - "D" - Other;
 - "E" - Alien student - restricted work authorized; and



○ "F" - Conditionally legalized alien.

- Foreign Born indicator (Citizenship code is not present, but individual was foreign born);
- State/country code;
- American Samoa indicator (True/False);
- Alien Registration Number (Alien Number or A-Number) (where applicable);
- Death indicator (Yes / No); and
- Error code descriptions (transaction and record levels).

The United States Citizenship and Immigration Services provides the following information to requesting agencies:

- Verification number (system generated);
- Initial request date;
- Identification type;
- Identification number;
- Last name;
- Benefit code;
- Benefit description;
- Initial request response (lawful status, no lawful status, deceased);
- Additional request date;
- Additional request response (lawful status, no lawful status, deceased);
- Third step request date;
- Third step resolution (lawful status, no lawful status, deceased); and
- Closed date.

The U.S. Citizenship and Immigration Services shares the following information to the U.S. Department of State:

- Full name;
- Date of birth;



- Social Security number; and/or
- U.S. passport number.

The U.S. Citizenship and Immigration Services may maintain the following information from the U.S. Department of State:

- Full name;
- Date of birth;
- Certificate of Citizenship;
- Certificate of Naturalization;
- Alien Registration Number (Alien Number or A-Number);
- U.S. passport book or passport card number;
- U.S. passport book or passport card issuance date;
- U.S. passport endorsement code(s) where applicable; and
- Images of U.S. passport book or passport card.

7. What is the intended use of personally identifiable information?

The SAVE Program uses personally identifiable information about individuals to help federal, state, territorial, tribal, and local government benefit-granting agencies, other authorized entities and licensing bureaus, as authorized by law, verify the citizenship and/or immigration status of individuals within their jurisdiction as they determine eligibility for benefits, credentials, and licenses; and verify voter registration. The U.S. Citizenship and Immigration Services also uses the personally identifiable information for federal security background investigations and other lawful purposes.

The U.S. Citizenship and Immigration Services uses a variety of data for cross-referencing. In this way, the U. S. Citizenship and Immigration Services ensures that data is accurate and current, identifies inconsistencies between or among databases, and minimizes fraud. Additionally, the U.S. Citizenship and Immigration Services collects personally identifiable information from individual users of the system to provide accountability of system usage in the event of misuse and abuse of the system. Further, the U. S. Citizenship and Immigration Services use personally identifiable information to register SAVE user agencies and other administration functions.

The U. S. Citizenship and Immigration Services will use the Social Security number from



requesting agencies to query the Social Security Administration Enumeration System to assist in providing U.S. citizenship or immigration status of individuals. Federal, state, local, tribal, and territory governments generally use the SAVE Program to assist in awards of benefits, voter registration verification, as well as identifying fraud.

The U.S. Citizenship and Immigration Services will compare U.S. passport information against information available in U.S. Department of State accessed systems to verify a match or no match. Using a passport number, the SAVE Program will be able to verify acquired or derived citizenship for individuals with a U.S. passport directly from the source records. Images of the U.S. Passport document may also be submitted by agencies when applicable to be used by status verifiers as part of the verification process. This ensures that personally identifiable information contained on the document can be used to verify the document and subsequently the citizenship status of the individual. Additionally, the U.S. Citizenship and Immigration Services will use U.S. passport application information, specifically, the Certificate or Citizenship or Certificate of Naturalization, to quickly verify citizenship status in certain cases and reduce its response time to registered users.

8. How long and under which retention schedule is the information retained?

Pursuant to the National Archives and Records Administration Authority N1-566-08-07, the U.S. Citizenship and Immigration Services maintains records within the SAVE Program for ten years from the date of the completion of the verification, unless the records are part of an ongoing law enforcement investigation in which case the U.S. Citizenship and Immigration Services may retain them until completion of the investigation.

9. With whom will personally identifiable information be shared?

Within the Component/Office

Specify:

Other-U.S. Department of Homeland Security Component(s)/Office(s)

Specify: When potential fraud or misuse is indicated by the SAVE Program information, this information may be shared, on a case-by-case basis, with U.S. Department of Homeland Security internal law enforcement organizations to include:

- U.S. Immigration and Customs Enforcement; and
- U.S. Customs and Border Protection.



<input checked="" type="checkbox"/> State, local, tribal, or territorial entities	Specify: A list of all requesting agencies and their purpose for accessing the SAVE Program is accessible at https://www.uscis.gov/save/save-agency-search-tool . Additionally SAVE may retrieve information from state driver’s license and identification issuing agencies (such as Department of Motor Vehicles).
<input type="checkbox"/> Public	Specify:
<input type="checkbox"/> Private sector	Specify:
<input type="checkbox"/> Foreign governments	Specify:
<input type="checkbox"/> Foreign entities	Specify:
<input checked="" type="checkbox"/> Other:	Specify: Social Security Administration, U.S. Department of State, and National organizations maintaining driver’s license and state identification information (such as the National Law Enforcement Telecommunications System).

10. How are individuals provided notice prior to the collection of information? If notice is not provided, explain why not.

Each registered agency completes a Memorandum of Agreement with the U.S. Citizenship and Immigration Services and agrees to provide notice to individuals within their jurisdiction of their use of information and sharing with the U.S. Citizenship and Immigration Services. Additionally, the U.S. Citizenship and Immigration Services provides notice through this Privacy Impact Assessment as well as system of records notices mentioned in Section 4. Each state holds the responsibility to provide notice of their use of information at the time of their collection or additional use of the information.

11. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out?

The U.S. Citizenship and Immigration Services does not provide opportunities to individuals within the jurisdiction of the registered agency to consent to the U.S. Citizenship and Immigration Services use of their information. Pursuant to the above-mentioned legal authorities



listed in Section 3, the U. S. Citizenship and Immigration Services must provide individual information to the Social Security Administration and the U.S. Department of State to allow the Requesting Agency to determine the immigration status of applicants and registrants of benefits, licenses, or for voter registration verification. Each registered agency holds the responsibility to provide opportunities for consent of their use of individuals' information. Additionally, each registered agency holds the responsibility to determine whether an individual has a legal right to decline providing information to them based on applicable law.

12. What procedures are in place to allow individuals to correct inaccurate or erroneous information?

Individuals may request access to their information maintained by the U.S. Citizenship and Immigration Services by submitting a request at <https://www.uscis.gov/records/request-records-through-the-freedom-of-information-act-or-privacy-act>.

Requesters are required to provide their Alien Registration Number and/or full name, date, and place of birth, and return address.

Individuals should provide all written requests to contest or amend their information reviewed by the SAVE Program, with appropriate proof of identity, class of admission, and other relevant identifying information, as well as a statement about the incorrect. Depending on the originating source of information, the request may be satisfied within the U.S. Citizenship and Immigration Services, or the individual may be referred to the appropriate record holding agency. If the source of data is from a U.S. Citizenship and Immigration Services download and the SAVE Program confirms the data is incorrect, often by comparing the documents with the information in the program and cross-referencing other U.S. Citizenship and Immigration Services Verification Information System databases, the SAVE Program will contact the appropriate system owner recommending that the data be corrected.²² Alternatively, the individual may make an appointment by calling the U.S. Citizenship and Immigration Services Contact Center at 800-375-5283 (TTY 800-767-1833). When appearing for the appointment, the person should provide accompanying supporting documentation, including proof of identity, class of admission, and other relevant identifying information. The SAVE Program customer agencies may change their profile information directly within the U.S. Citizenship and Immigration

²² The Verification Information System is a composite information system incorporating data from various U.S. Department of Homeland Security and Social Security Administration databases and functions as the underlying information technology that supports the SAVE Program. The Verification Information System supports the U.S. Citizenship and Immigration Service's ability to verify whether a newly hired employee is authorized to work in the United States and the citizenship or immigration status verification of individuals seeking certain government benefits. The Verification Information System, including the services it houses, is in the Amazon Web Service cloud environment.



Services Verification Information System application. To correct typographic errors in your U.S. Citizenship and Immigration Services record or document, visit egov.uscis.gov/e-request.

13. What administrative, technical, and physical controls are used to protect the information?

The SAVE Program requires potential enrollees and customer agencies to register for participation in the program and sign an appropriate data sharing agreement. Once the enrollees submit the required documentation, all users must complete a web-based training course that explains functionality and security requirements.

The Systematic Alien Verification for Entitlements Program's internal users take the mandatory annual U.S. Department of Homeland Security Computer Security Training and the U.S. Citizenship and Immigration Services Privacy Awareness Training. Additionally, staff who administer the SAVE Program are required take special, role-based training. External SAVE Program users complete online tutorials. The tutorials also cover the procedures and policies associated with the use of the SAVE Program and includes privacy-related topics.

The Verification Information System, as the underlying technology supporting the SAVE Program has been Certified and Accredited and received a full authority to operate in April 2014. The system has been approved to participate in the Ongoing Authorization process and is continually monitored for compliance with the National Institute of Science and Technology policies to ensure compliance with the Federal Information System Management Act. The SAVE Program implements access controls for both internal and external customers, such as account names and passwords to access the program. The program has an automated mechanism to ensure that users change their passwords at specified intervals. Additionally, the program implements the following technical controls:

- Password data is encrypted within the system;
- The system is located within a multi-layered firewall architecture;
- The system follows a robust set of security controls that meet the U.S. Department of Homeland Security System Security Policy requirements. The certification and accreditation process ensures that the U.S. Citizenship and Immigration Services documents and verifies these security controls through the certification and accreditation process;
- The system uses secure hypertext transfer protocol protected communications during all data transmissions between the client workstation and the system;



- Passwords are encrypted when making database connections; and
- Procedures are in place to ensure that any potential breaches of information are reported within one hour of being found.

14. How does the Component ensure that personally identifiable information is used appropriately?

The SAVE Program has a comprehensive audit trail tracking and maintenance function that stores information about users who submit queries, when the query was processed, the query response, who received the query response, and when the user received the query response. The audit logs have restricted access based on user roles. These logs are external to system administration access methods and protected from modification. U.S. Citizen and Immigration Services personnel periodically review these audit logs to monitor user activity. Registered agencies must abide by all security requirements that they agreed to when they enrolled in the program. Attempts to evade the security controls can result in loss of access to the SAVE Program.

Some registered agencies use a single sign-on for all their individual users. In these cases, the SAVE Program will not collect information from individual users because individual users will appear as one agency user. In the case of single sign-on access to users, the U.S. Citizenship and Immigration Services requires the agency to sign an addendum to their Memorandum of Agreement which states that every user of the system must be assigned a unique identifier. If requested, the agency provides this information to the U.S. Citizenship and Immigration Services to allow for a clear audit trail for all transactions.

Associated Privacy Risks and Mitigations

Privacy Risk:	There is a risk that the U.S. Citizenship and Immigration Services may share inaccurate information with registered agencies, which could in turn impact a registered user agency’s eligibility determination for an individual.
Mitigation:	The U.S. Citizenship and Immigration Services partially mitigates this risk. Generally, the SAVE Program has a 3-step process. The first step is a general query of the system. However, due to misspelling of names, transposed numbers, or incomplete information, the SAVE Program may produce inaccurate results. To mitigate this, the SAVE Program has a manual step process where a U.S. Citizenship and Immigration Services staff member will try to reconcile the request manually. The third step is for



Homeland Security

Privacy Impact Assessment
DHS/USCIS/PIA-006(d) SAVE
Page 20

	<p>the U.S. Citizenship and Immigration Services to get additional documentation from the registered agency. However, this only partially mitigates the risk since the new request using Social Security numbers does not allow for a second and third step review. The U.S. Citizenship and Immigration Services does not have direct access to the Social Security Administration system to support these additional steps. Additionally, registered agencies may not go through all steps to ensure accuracy of information.</p>
<p>Privacy Risk:</p>	<p>There is a risk that all United States citizens, including natural born U.S. citizens, have not been provided notice that the SAVE Program collects or maintains their information for citizenship and immigration status.</p>
<p>Mitigation:</p>	<p>The United States Citizenship and Immigration Services partially mitigates this risk. It is the responsibility of each registered agency to provide notice to individuals within their jurisdiction of their use of information and sharing with the U.S. Department of Homeland Security/U.S. Citizenship and Immigration Services. The U.S. Citizenship and Immigration Services is publishing this privacy impact assessment and related System of Records Notice to provide transparency regarding the new categories of information collected and shared to assist registered agencies in verifying citizenship and immigration status of individuals applying for a benefit or license and voter registration verification. The SAVE Program's "Register an Agency for SAVE" explains how an eligible agency can create a Memorandum of Agreement with the U.S. Citizenship and Immigration Services. These agreements require registered user agencies to comply with the Privacy Act of 1974, 5 U.S.C. § 552a, as amended, and other applicable laws, regulations, and policies. These policies include transparency and notice to individuals regarding agencies collection and use of personally identifiable information.</p>
<p>Privacy Risk:</p>	<p>There is a risk that the U.S. Citizenship and Immigration Services may use the information it obtains from registered agencies, the Social Security Administration, and the U.S. Department of State, for purposes not authorized by statute or for which it was originally collected.</p>
<p>Mitigation:</p>	<p>The United States Citizenship and Immigration Services mitigates this risk by only collecting information as authorized by the Immigration and Naturalization Act and other authorities mentioned within this Privacy</p>



Homeland Security

	<p>Impact Assessment. The purpose for sharing Social Security numbers with the Social Security Administration and receiving information is to allow user agencies to verify the citizenship or immigration status of individuals applying for a benefit, license, or voter registration verification. The purpose for sharing and receiving U.S. passport information with the U.S. Department of State is to verify the citizenship or immigration status of individuals applying for a benefit, license or for voter registration verification. Also, each registered agency must execute a Memorandum of Agreement or Computer Matching Agreement with the U.S. Citizenship and Immigration Services that includes terms that the SAVE Program will be used in accordance with the law.</p>
--	--

Privacy Risk:	<p>There is a risk that the new category individuals covered by this assessment/notice, specifically, United States born citizens do not have the opportunity to individually participate or consent in how the U.S. Citizenship and Immigration Services uses their information.</p>
Mitigation:	<p>The U.S. Citizenship and Immigration Services cannot mitigate this risk. Each user agency is responsible for complying with federal and local authorities. The U.S. Citizenship and Immigration Services assumes that each user agency factors in the principles of notice, individual participation, and consent prior to providing information to the U.S. Citizenship and Immigration Services. The U.S. Citizenship and Immigration Services only uses the information for the authorized purpose(s) identified within this Privacy Impact Assessment. Individuals should consult their local government agencies to determine the appropriate opt-in or opt-out statute, regulations and policies.</p>

Privacy Risk:	<p>There is a risk that individuals may access the SAVE Program that do not have a need to know of the information.</p>
Mitigation:	<p>The U.S. Citizenship and Immigration Services mitigates this risk by requiring the SAVE Program’s potential enrollees and customer agencies to register for participation in the program and sign a Memorandum of Agreement or Computer Matching Agreement. After all required documentation is submitted, all users must complete a web-based training course that explains functionality and security requirements.</p> <p>The SAVE Program’s internal users complete the mandatory annual privacy</p>



Homeland Security

	and information technology training. External program complete take on-line tutorials explaining the program. The tutorials also cover the procedures and policies associated with the use of the program.
--	--

Contact Official

Brian Broderick
Division Chief (Acting)
Verification Division
U.S. Citizenship and Immigration Services

Responsible Official

Angela Y. Washington
Component Privacy Officer
Office of Privacy
U.S. Citizenship and Immigration Services
U.S. Department of Homeland Security
USCIS.PrivacyCompliance@uscis.dhs.gov

Approval Notice:

By signing below, the U.S. Department of Homeland Security Chief Privacy Officer approves this Privacy Impact Assessment for the SAVE Program. If, however, during the operational course of this program or U.S. Citizenship and Immigration Services' use of this technology changes from what has been documented or the U.S. Department of Homeland Security Privacy Office becomes aware of evidentiary changes to the intended use of the personally identifiable information or the scope of the personally identifiable information collected, of the program or technology is determined to be ineffective, the Chief Privacy Officer reserves the right to revoke approval of this Privacy Impact Assessment.

Approval Signature

Original, signed copy on file with the U.S. Department of Homeland Security Privacy Office.

Roman Jankowski
Chief Privacy Officer
U.S. Department of Homeland Security
Privacy@hq.dhs.gov

Exhibit 14



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 1 of 42

PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals, and to assess whether there is a need for additional privacy compliance documentation or requirements. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used. In accordance with the Fair Information Practice Principles (FIPPs),¹ Component Privacy Officers should consider best practices for privacy safeguards and principles when reviewing and adjudicating PTAs.

Please complete the attached PTA and submit it to your Component Privacy Office. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

The Component or DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If privacy compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement/Privacy Notice, or Computer Matching Agreement (CMA) – the Component Privacy Office will send you a copy of the relevant compliance template to complete and return.

¹ See [The Fair Information Practice Principles | Homeland Security](#).



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 2 of 42

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	Systematic Alien Verification for Entitlements Program		
Component or Office:	U.S. Citizenship and Immigration Services (USCIS)	Office or Program:	Verification Division
FISMA Name (if applicable):	Verification Information System	FISMA Number (if applicable):	CIS-06285-MAJ-06285
Type of Project or Program:	System	Project or program status:	Operational
Date first developed:	July 7, 2007	Pilot launch date:	N/A
Date of last PTA update	February 7, 2023	Pilot end date:	N/A
ATO Status (if applicable):²	Complete	Expected ATO/ATP/OA date (if applicable):	Ongoing Authorization

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	Irina Sidelnikov		
Office:	Office of Information Technology	Title:	OIT Project Manager
Phone:	[REDACTED]	Email:	[REDACTED]

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Minh Vo		
Phone:	N/A	Email:	[REDACTED]

² The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see <https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Documents/DHS%20ATP%20Guide%20v2.0.pdf#search=atp>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 3 of 42

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

The United States Citizenship and Immigration Services submits this updated Privacy Threshold Analysis to document the United States Citizenship and Immigration Services Verification Division and Office of Technology changes to the Systematic Alien Verification for Entitlements Program. The United States Citizenship and Immigration Services administers the Systematic Alien Verification for Entitlements Program, an inter-governmental initiative that provides a web-based service to help federal, state, territorial, tribal and local agencies and other governmental entities verify United States citizenship or immigration status/category information of applicants for benefits, licenses, or other authorized purposes.

This Privacy Threshold Analysis documents that the Systematic Alien Verification for Entitlements Program has

1. Expanded its search capabilities to allow approved Systematic Alien Verification for Entitlements Program user agencies to verify United States citizenship information using Social Security Numbers and other non-Department of Homeland Security enumerators.
2. A new Social Security Administration system connection to support verification of citizenship/immigration status.
3. A new bulk uploader/list processor function that allows user agencies to upload lists of benefit applicants.
4. Use of the Voter Registration and Voter List Maintenance Verification functionality.
5. The collection of information from the Department of State's Consular Consolidated Database/American Citizen Record Query system. Additionally, the Systematic Alien Verification for Entitlements Program will integrate with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data system.

2025 Updates

On April 22, 2025, Homeland Security Secretary Kristi Noem, alongside the United States Citizenship and Immigration Services and the Department of Government Efficiency, announced a comprehensive optimization of the Systematic Alien Verification for Entitlements Program to ensure a single, reliable source for verifying immigration status and United States citizenship nationwide. Congressional, federal, and state stakeholders have periodically expressed interest in using the Systematic Alien Verification for Entitlements to verify naturalized and derived citizenship information during voter registration and/or for voter list maintenance. Verification for voter list maintenance purposes often occurs when a state Department of Motor Vehicles compares its records to state voter agency records to determine if individuals on the voter rolls represented that they were other than U.S. citizens when the Department of Motor Vehicles issued their driver's license. The state voter agency then follows up with those individuals as to their citizenship status through state law voter registration challenge procedures. The United States Citizenship and Immigration Services Verification Division is leading this effort and has identified multiple phases to optimize the program. A high-level summary is provided below, while a more detailed description of each phase follows.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 4 of 42

- Phase 1: Free Service for State, Local, Tribal, Territory agencies and Bulk Uploader. (Estimated completion: Implemented)
- Phase 2: Integration with the Social Security Administration to allow for full Social Security Number to be used as a non-Department of Homeland Security enumerator. (Estimated completion: Implemented)
- Phase 3: Modify the Security Administration integration to allow for truncated Social Security Numbers (last 4-digits) to be used as a non-Department of Homeland Security enumerator. (Estimated completion: July/August 2025)
- Phase 4: Integration with Customs and Border Protection to enable United States passport data, received from the Department of State, to be used within the Systematic Alien Verification for Entitlements Program. (Estimated completion: To be determined)
- Phase 5: Integration with the Department of Justice to enable an incarceration/felony related flag (the flag will be used internally and will not be sent to the agencies or the applicants). (Estimated completion: To be determined)
- Phase 6: Integration with State Driver's Licensing Agencies to enable a Driver License number to be used as a non-Department of Homeland Security enumerator. (Estimated completion: To be determined)

The summary below focuses on phases one (1) through four (4). More detailed information can be found later in this document. Phases five (5) and six (6) are longer term goals of the optimization effort and are still in the exploratory/planning stage. The United States Citizenship and Immigration Services will update this Privacy Threshold Analysis to support the remaining phases during their development.

Phases One (1) through Three (3)

Systematic Alien Verification for Entitlements Program eliminated fees for non-federal users creating Systematic Alien Verification for Entitlements Program cases. User agencies can now create multiple individual cases from a list of data provided by the user. Further, the Systematic Alien Verification for Entitlements Program plans to integrate additional immigration information into search functionality and case results, such as timelines and addresses. Improved automatic status updates and a new user-friendly interface will empower federal, state, local, territorial, and tribal agencies to help prevent individuals who are not qualified for government benefits and licenses from receiving those benefits and licenses. The Department of Homeland Security intends to provide ongoing updates to stakeholders as the Systematic Alien Verification for Entitlements Program Optimization Plan progresses. Systematic Alien Verification for Entitlements Program users must attest to completing the Systematic Alien Verification for Entitlements Program tutorial prior to gaining access to Systematic Alien Verification for Entitlements Program. Users' access is based on their permissions.

The United States Citizenship and Immigration Services has developed and implemented a new bulk uploader/list processor feature to the Systematic Alien Verification for Entitlements Program. This feature will allow program users to upload a list (such as an excel spreadsheet) of benefit applicants to the Systematic Alien Verification for Entitlements Program for processing. Once the list is uploaded, the Systematic Alien Verification for Entitlements Program will accept or not accept the data then, through an automated process, create front-end single-record cases for each entry. Initially the creation of cases using this feature is limited to cases created using an A-number, Citizenship or Naturalization Certificate



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 5 of 42

number, or Social Security number. Agencies will not be prompted to institute additional verification when using this process but are instructed to resubmit additional information when the process is unable to return a response. Expansion of this feature in the future may include the ability to create cases with additional enumerators and the ability to request configured information not automatically selected for the benefit type.

User agencies will be able to access each case created using the list processor feature in the Systematic Alien Verification for Entitlements system as normal, by viewing the individual case status and response. The Systematic Alien Verification for Entitlements Program also has a feature available to all the user agencies to generate a report that will list all the cases created, the status of the case and the Systematic Alien Verification for Entitlements Program response. Access to generate the report, including what cases are included, will vary depending upon the individual user's permission. United States Citizenship and Immigration Services is providing this verification service for all benefit requests. There are approximately 1,200 user agencies with access to the Systematic Alien Verification for Entitlements Program to verify immigration status for benefits or entitlements, and in fiscal year 2024, the Systematic Alien Verification for Entitlements Program completed over 24.5 million first step verifications.

The Systematic Alien Verification for Entitlements Program was originally designed only to use a Department of Homeland Security-issued enumerator (such as an alien number or A-Number) to query immigration records, specifically, to provide immigration status to Systematic Alien Verification for Entitlements Program user agencies. The Systematic Alien Verification for Entitlements Program is now expanding to allow Systematic Alien Verification for Entitlements Program user agencies to provide a Social Security Number or a United States Passport number to query the Systematic Alien Verification for Entitlements Program.

The Systematic Alien Verification for Entitlements Program will also add the ability for user agencies to verify truncated Social Security Numbers (last 4 digits) against Social Security Administration records. This will allow the Systematic Alien Verification for Entitlements Program to verify all United States citizens including those by birth, which was previously not available. A benefit applicant's Social Security number can only be used for automated initial verification and cannot be used for additional verification, which will continue to require a Department of Homeland Security immigration enumerator since the Systematic Alien Verification for Entitlements Program does not normally collect Social Security Numbers or passport numbers. The addition of the Voter Registration and Voter List Maintenance Verification, and the Social Security Administration connection is now live. The Systematic Alien Verification for Entitlements Program can now verify United States-born citizens for voter verification agencies.

The Department of Homeland Security/United States Citizenship and Immigration Services seeks access to Social Security Administration information accessed through the Department of Homeland Security/United States Citizenship and Immigration Services Verification Information System³. The United States Citizenship and Immigration Services and the Social Security Administration agreed to the following limitations on the access to, and disclosure and use of information that identifies a verification request as being generated by United States Citizenship and Immigration Services or associated with a United States Citizenship and Immigration Services program:

³ Verification Information System provides services to customers through Systematic Alien Verification for Entitlements and E-Verify (the latter of which will not be used for this initiative).



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 6 of 42

- Data or information that identifies a verification request as being generated by United States Citizenship and Immigration Services or associated with a United States Citizenship and Immigration Services program will remain information owned by United States Citizenship and Immigration Services.
- The United States Citizenship and Immigration Services will use the verification responses generated by the Social Security Administration only for the purposes described in the Information Sharing Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services and the Social Security Administration.
- Data or information that identifies a verification request as being generated by the United States Citizenship and Immigration Services or associated with a United States Citizenship and Immigration Services program will be used only as provided in the Information Sharing Agreement by the Social Security Administration.
- Data or information that identifies a verification request as being generated by United States Citizenship and Immigration Services or associated with the United States Citizenship and Immigration Services program provided by Social Security Administration will not be duplicated or disseminated outside Social Security Administration without prior written approval from United States Citizenship and Immigration Services. The United States Citizenship and Immigration Services will not give such approval unless the redisclosure is required by law or is essential to the conduct of the exchange. In such cases, the Social Security Administration, the agency redisclosing the records, must specify in writing what records will be redisclosed, to whom they will be redisclosed, and the reasons that justify redisclosure.
- The United States Citizenship and Immigration Services will not duplicate or disseminate the verification responses for a purpose not covered by the Information Sharing Agreement, within or outside of its agency, without the written permission of the Social Security Agreement excepted as required by Federal law. The Social Security Administration will not give such permission, unless Federal law requires disclosure, or disclosure is essential to the purpose of this Agreement. For such permission, The United States Citizenship and Immigration Services must specify in writing what data it is requesting to duplicate or disseminate and to whom, and the reasons that justify such duplication or dissemination.

Administrative Safeguards

The Social Security Administration and the United States Citizenship and Immigration Services will restrict access to the data matched and to any data created by the match to only those users, for example, employees and contractors, who need it to perform their official duties in connection with the uses of the data authorized in the Information Sharing agreement. Further, the Social Security Administration and the United States Citizenship and Immigration Services will advise all personnel with access about the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws.

Parties, including all personnel with access to information, will be appropriately educated and trained regarding the proper handling of personally identifiable information and proper care of the information systems to ensure the overall safeguarding and security of the information. The Social Security Administration and the United States Citizenship and Immigration Services will ensure that its



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 7 of 42

employees, including contractors with the access to any of the information, have completed privacy training on the handling of personally identifiable information.

Phase Four (4)

The United States Citizenship and Immigration Services will need to query other non-United States Citizenship and Immigration Services systems, besides the Social Security Administration's Numident system, with the information provided by the Systematic Alien Verification for Entitlements Program user agency to find the appropriate Department of Homeland Security-issued enumerator to continue with the Systematic Alien Verification for Entitlements Program case processing. For instance, USCIS is researching the possibility of using a United States Passport Number to be able to identify a Department of Homeland Security-issued enumerator. In a case when a User Agency uploads or enters a United States Passport Number instead of a DHS-issued enumerator, the Systematic Alien Verification for Entitlements Program will query another non-United States Citizenship and Immigration Services System using the United States Passport Number along with a unique identifier to find any records and will identify if a Department of Homeland Security-issued enumerator was used by the applicant when applying for a Department of Homeland Security-issued benefit or if a Passport Number was used at a United States Port of Entry and is associated with a Department of Homeland Security-issued enumerator. In this instance, to enable this change, the Systematic Alien Verification for Entitlements Program would integrate with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data to match a Passport Number against Customs and Border Protection and Department of State records to attempt to locate a Department of Homeland Security issued enumerator.

The TECS (not an acronym) - Travel Documents and Encounter Data stores travel document information (scanned images of documents, biographic information, document details, and photographs) from the United States Citizenship and Immigration Services Lawful Permanent Resident Cards along with Department of State-issued United States passports, visas, foreign passports, enhanced driver's licenses, and enhanced tribal cards. The TECS (not an acronym) - Travel Documents and Encounter Data USPassportRESTService allows interconnected systems to query TECS (not an acronym) - Travel Documents and Encounter Data for United States passport information. For this use case, the Systematic Alien Verification for Entitlements Program user agency will input a passport number into the Systematic Alien Verification for Entitlements Program. The query will trigger the USPassportRESTService to locate the matching United States passport number and return the results to the user. This will allow the Systematic Alien Verification for Entitlements Program to verify all types of United States citizens, including those by birth, which was previously not available. Currently, the Systematic Alien Verification for Entitlements Program only collects passport numbers for foreign issued passports if it is provided with an additional Department of Homeland Security enumerator. The United States Citizenship and Immigration Services E-Verify has an existing connection to the USPassportRESTService, which also resides within the Verification Information System, like Systematic Alien Verification for Entitlements Program.

The following are updates that were planned prior to Secretary Noem's vision for optimizing the Systematic Alien Verification for Entitlements Program and are still in progress.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 8 of 42

- Systematic Alien Verification for Entitlements Program will update the responses provided to users as part of the Interface Control Agreement Version 38, which enhances the Systematic Alien Verification for Entitlements Program query logic to provide more accurate information based on the need to know. The Systematic Alien Verification for Entitlements Program will add the collection of an uploaded document such as a Naturalization/Citizenship Certificate Number, when the user submits a second step additional verification, as well as the collection of a reason code, which allows the Systematic Alien Verification for Entitlements Program users to provide additional details regarding the applicant's request, particularly during the additional verification process. The Systematic Alien Verification Entitlements responds to users by providing an immigration status/category or United States citizenship. These additional collections will help Systematic Alien Verification for Entitlements Program identify and remedy data issues, reduce overall manual response times, and allow the Systematic Alien Verification for Entitlements Program to improve the quality of first step automated responses.
- A live site environment will be implemented where Systematic Alien Verification for Entitlements web service users can access new and current interface control agreements. This will streamline the process to update the interface control agreements and ensure that the Systematic Alien Verification for Entitlements Program users have access to the most current information for the Interface Control Agreement Version 38.
- The Systematic Alien Verification for Entitlements Program case response screen will be redesigned so that it is easier to read and allow for the additional information to be submitted. The screen will be packaged in a new way to provide the user clear information during the initial verification.

Additionally, Systematic Alien Verification for Entitlements Program will be collecting information from the Department of State's Consular Consolidated Database / American Citizen Record Query system which is a consular search engine used by the Department of State to manage and access records related to United States citizens, particularly for consular protection and services, including managing passport requests and applications.

2024 Update

As part of the Systematic Alien Verification for Entitlements Program's normal review process, the United States Citizenship and Immigration Services intends to access the Department of State's Consular Consolidated Database / American Citizen Record Query system to verify immigration status of applicants for benefits, licenses, and other authorized purposes. The purpose of collecting this information is to confirm the identity of the applicant to determine their status. This process is part of an ongoing effort that began in 2024.

Background

The Systematic Alien Verification for Entitlements Program is an online service for registered federal, state, territorial, tribal, and local government agencies to verify immigration status and United States citizenship of applicants seeking benefits or licenses. Systematic Alien Verification for Entitlements



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 9 of 42

Program is not a database but queries Department of Homeland Security-accessed federal records to provide registered user agencies with a verification response.

In 1986, Congress mandated that the Immigration and Naturalization Service, now United States Citizenship and Immigration Services, establish a system to verify the citizenship and immigration status of individuals seeking government benefits and licenses.

The United States Citizenship and Immigration Services Verification Division administers the Systematic Alien Verification for Entitlements Program, which is an intergovernmental initiative using a web-based service to help federal, state, territorial, tribal and local benefit-issuing and licensing agencies and other governmental entities determine the immigration status or United States citizenship of applicants for public benefits, licenses, grants, credentials, background investigations, and other lawful purposes, so only entitled applicants receive them. Systematic Alien Verification for Entitlements Program verifies immigration status/category and United States citizenship against Department of Homeland Security-accessed records. Historically, the Systematic Alien Verification for Entitlements Program has not verified information for United States born citizens as a Department of Homeland Security immigration enumerator was previously required, but now the Systematic Alien Verification for Entitlements Program can verify United States-born United States citizens against Social Security Administration data. The Systematic Alien Verification for Entitlements Program does not determine an applicant's eligibility for a specific benefit or license, as this is the responsibility of the benefit/license granting agency.

As of April 1, 2025, the Systematic Alien Verification for Entitlements Program has revised its transaction charges for all state, local, tribal, and territorial government agencies using the Systematic Alien Verification for Entitlements Program to eliminate those charges. Federal agencies are still charged a fee to use the Systematic Alien Verification for Entitlements Program. The authority for the Systematic Alien Verification for Entitlements Program, and for particular Systematic Alien Verification for Entitlements Program authorized uses can be found in the Immigration Reform and Control Act⁴; the Personal Responsibility and Work Opportunity Reconciliation Act⁵ Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996⁶, and the REAL ID Act of 2005⁷, the Patient Protection and Affordable Care Act of 2010,⁸ and the Federal Aviation Administration Extension, Safety and Security Act of 2016.⁹ In addition, the Systematic Alien Verification for Entitlements Program has an obligation under 8 U.S.C. 1373(c) to "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."

⁴ Immigration Reform and Control Act of 1986, Public Law No. 99-603

⁵ Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Public Law No. 104-193, 110 Statute 2168

⁶ Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 Public Law 104-208, 110 Statute 3009

⁷ REAL ID Act of 2005, Public Law No. 109-13, 119 Statute 231

⁸ Patient Protection and Affordable Care Act of 2010, Public Law No. 111-148

⁹ Federal Aviation Administration Extension, Safety and Security Act of 2016 (Federal Aviation Administration Act), Public Law No. 114-190 § 3405(d) (July 15, 2016).



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 10 of 42

The United States Citizenship and Immigration Services Verification Division operates the Verification Data Information System as the search engine for Systematic Alien Verification for Entitlements Program and the E-Verify Program. The Verification Data Information System accesses nationally accessible databases of selected immigration records to support both the Systematic Alien Verification for Entitlements Program and the E-Verify Program. The Systematic Alien Verification for Entitlements Program queries an individual's immigration status to help the administering agency determine eligibility for any public benefit, license, or credential based on their United States citizenship or immigration status. The United States Citizenship and Immigration Services is obligated by law to 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.

Systematic Alien Verification for Entitlements Program

The United States Citizenship and Immigration Services administers the Systematic Alien Verification for Entitlements Program, an inter-governmental initiative that provides a web-based service to help federal, state, territorial, tribal, and local benefits-issuing and licensing agencies and other governmental entities along with Airport Operators verify the United States citizenship and immigration status/category information of applicants for public benefits or licenses (hereinafter "benefits"). Examples of these benefits include Supplemental Security Income Supplemental Nutrition Assistance Program (formerly food stamps), Temporary Assistance for Needy Families cash assistance, Medicaid, Children's Health Insurance Program, REAL ID compliance, and other statutorily authorized purposes, including voter verification.

The Systematic Alien Verification for Entitlements Program also eliminates fees for database searches, breaks down silos for more accurate results, streamlines List Processor submission, and integrates additional immigration information, such as timelines and addresses. Automatic status updates and a new user-friendly interface will empower Federal, state, local, territorial, and tribal agencies to help prevent individuals who are not qualified for government benefits from receiving those benefits. The Department of Homeland Security intends to provide ongoing updates to stakeholders as the Systematic Alien Verification for Entitlements Program Optimization Plan progresses.

Agency use of the Systematic Alien Verification for Entitlements Program is administered by the Verification Division. All user agencies are required to register with the Systematic Alien Verification for Entitlements Program to access the system prior to using the Systematic Alien Verification for Entitlements Program. The Systematic Alien Verification for Entitlements Program is not a source system and connects with federal immigration systems, and now the Social Security Administration's Numident¹⁰ system, to access applicable information. The Systematic Alien Verification for Entitlements Program also has a Case Status Check capability that allows benefit applicants to view the status of their Systematic Alien Verification for Entitlements Program case. The system provides benefit eligibility checks based on the grant dates. The Verification Division has a three (3) tier process when verifying an individual's immigration status or United States citizenship.

¹⁰ NUMIDENT or "Numerical Identification" refers to the master file of Social Security Administration records containing information about individuals who have applied for or been assigned a Social Security Number. This file includes records for applications, claims, and death records related to individuals with a Social Security Number.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 11 of 42

Users must perform all additional verification procedures the Systematic Alien Verification for Entitlements Program requires and/or the applicant requests prior to denying a benefit based upon a Systematic Alien Verification for Entitlements Program response. Users must provide all applicants who are denied benefits based solely or in part upon the Systematic Alien Verification for Entitlements Program response adequate written notice and the information necessary to contact the Department of Homeland Security so that applicants may correct their immigration records in a timely manner, if necessary.

Initial verification

A Systematic Alien Verification for Entitlements Program user agency accesses their account in the system and either submits requests individually or via a bulk request using the system's new bulk uploader feature. When a Systematic Alien Verification for Entitlements Program user agency submits an online verification request for a benefit applicant, it provides several required identifiers for the benefit applicant from documents presented by the benefit applicant, including first and last name, date of birth, and at least one of the following: an enumerator from the Department of Homeland Security (e.g. Alien number/United States Citizenship and Immigration Services number, Form I-94 Number, Card Number/I-797 Receipt number, Citizenship/Naturalization Certificate Numbers), a Social Security number from Social Security Administration, or a United States passport number from the Department of State. Social Security Numbers and United States passport numbers are new enumerators. Previously, enumerators were solely limited to Department of Homeland Security-issued immigration enumerators.

In the case of a bulk upload the Systematic Alien Verification for Entitlements Program will use an automated process to create individual cases for each benefit applicant on the list.

Using these data fields, the Systematic Alien Verification for Entitlements Program performs an automated query of various Systematic Alien Verification for Entitlements Program-accessed federal databases for relevant records. If a Social Security Number is submitted under this new collection, the Systematic Alien Verification for Entitlements Program will verify this enumerator against the Social Security Administration records, including the Social Security Administration death records and citizenship records. If the individual's Social Security account has a record of an A-number or certificate number, the Social Security Administration will provide that information to the Systematic Alien Verification for Entitlements Program, which will be used to validate that information against the Department of Homeland Security records. If a United States passport number is submitted, the Systematic Alien Verification for Entitlements Program will verify it against the Department of State related records available in the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data system. When the Systematic Alien Verification for Entitlements Program locates a record pertaining to the benefit applicant in any of these federal databases, the Systematic Alien Verification for Entitlements Program displays a verification response to the user agency within seconds.

Second step, additional verification (Tier 2)



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 12 of 42

If the Systematic Alien Verification for Entitlements Program is unable to find a record pertaining to the benefit applicant through the automated first level search of the Department of Homeland Security records, including United States passport records and the Social Security Administration records, it displays a response to the user indicating additional action is required from the user agency, including requesting additional verification when an immigration enumerator is available. If only a Social Security Number is submitted for verification, the user agency will be informed to close the case and submit a new request using either corrected data or an immigration enumerator, since additional verification cannot be conducted with only a Social Security Number.

The Systematic Alien Verification for Entitlements Program user agency may start the additional verification procedure, which may include is an in-depth manual review by Systematic Alien Verification for Entitlements Program staff (Status Verification Analyst) to determine the applicant's immigration status or United States citizenship. At the point at which the "Institute Additional Verification" message is displayed, user agencies must submit the case for additional verification if they are relying on a Systematic Alien Verification for Entitlements Program response to deny a benefit. Additionally, if the user agency receives a response and they have questions about the validity of the response, the user agency may submit a case that already received a Systematic Alien Verification for Entitlements Program response for additional verification. Users must also submit a case for additional verification when requested by the applicant.

User agencies may not rely on a Systematic Alien Verification for Entitlements Program response to approve or deny an application for benefits unless they have followed all required Systematic Alien Verification for Entitlements Program verification procedures. The Systematic Alien Verification for Entitlements Program users are not required to institute additional verification if a user agency has alternate grounds upon which to base its decision to decide a benefit that do not require verification of the applicant's immigration status/category, even where the agency is prompted to do so. Examples of when a user agency has alternate grounds to base a decision that does not require the completion of additional verification include:

- The applicant does not meet eligibility requirements for the benefit unrelated to immigration status/United States citizenship.
- The applicant withdraws their application.
- The applicant cannot be contacted/fails to respond to an agency's request for follow-up.
- The applicant presents documentation the Systematic Alien Verification for Entitlements Program cannot verify (such as a military identification).

This revision adds the collection of an uploaded document which includes immigration enumerators (such as a Form I-94, Arrival/Departure Records, Naturalization/Citizenship Certificate, or passport records) when a case is submitted for second step additional verification as well as a reason code. Reason codes can provide information on why the initial verification was not successful, if the case has been escalated for additional verification, or suggest that additional verification steps may be needed to determine the applicant's status or eligibility for a benefit. Reason codes can also identify if it was a user-initiated additional verification request when the user received an initial Systematic Alien Verification for Entitlements Program response providing an immigration status/category or United States citizenship. These additional collections will help the Systematic Alien Verification for Entitlements Program identify



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 13 of 42

and remedy data issues, reduce overall manual response times, and allow the Systematic Alien Verification for Entitlements Program to improve the quality of first step automated responses.

If the second step manual search produces relevant information enabling the verification of immigration status, the Systematic Alien Verification for Entitlements Program provides an electronic response to the inquiring user agency.

If the user agency declines second step additional verification, the verification process ceases. Additional screens notify the user agency that closing the case without performing additional verification means the agency does not have a complete Systematic Alien Verification for Entitlements Program response. The Systematic Alien Verification for Entitlements Program user agencies cannot rely upon an incomplete Systematic Alien Verification for Entitlements Program response to deny a benefit.

Third step Additional Verification with Documents (Tier 3)

If a benefit applicant's immigration status/category cannot be verified on initial or additional verification step when submitting a Department of Homeland Security enumerator, the system will prompt the user agency to resubmit the case with documents. When the prompt is received, the agency must upload a copy of the front and back of the immigration document the applicant presented to the user agency for the Systematic Alien Verification for Entitlements Program to perform detailed manual research at third step. A Department of Homeland Security immigration enumerator is required for the third step additional verification. The Systematic Alien Verification for Entitlements Program cannot complete third step additional verification using non-immigration documentation. The Systematic Alien Verification for Entitlements Program user agencies are legally authorized to make electronic copies of immigration documents for purposes of verifying immigration status. Cases created with just the Social Security Number or a Passport Number as the enumerator are not subject to this step.

If the third step manual review produces relevant information enabling the verification of immigration status/category or United States citizenship, the Systematic Alien Verification for Entitlements Program provides an electronic response to the user agency.

If a benefit applicant's immigration status/category is not verified after completing third step verification, the Systematic Alien Verification for Entitlements Program will provide additional information or guidance on how to proceed.

If the applicant believes their information in the Department of Homeland Security records is incorrect, the applicant can seek a records correction. User agencies should provide the Systematic Alien Verification for Entitlements Program Fact Sheet and Systematic Alien Verification for Entitlements Program Records: Fast Facts for Benefit Applicants¹¹ to benefit applicants that may require records correction.

¹¹ The Systematic Alien Verification for Entitlements Fact Sheet and Systematic Alien Verification for Entitlements Records: Fast Fact for Benefits Applicants is accessible at <https://www.uscis.gov/save/benefit-and-license-applicants/resources-for-benefit-and-license-applicants>



The Systematic Alien Verification for Entitlements Program user agency continues to have the option of running a web report within the system that will create a file in Adobe format of all cases processed for their organization. The United States Citizenship and Immigration Services provides access to relevant reports of approved or pending cases for Systematic Alien Verification for Entitlements Program user agencies to assist them in managing their Systematic Alien Verification for Entitlements Program cases and monitoring their own compliance with the Systematic Alien Verification for Entitlements Program rules and the federal deeming and reimbursement rules. User agencies can run case-specific reports for quality assurance that will include information, such as name, date of birth, type of benefit, immigration identifier (e.g., A-Number, unexpired foreign passport number, I-94 Arrival/Departure Record), and immigration status, only if the benefit was administered.

Voter Registration and Voter List Maintenance Verification

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 expanded the Systematic Alien Verification for Entitlements Program by requiring the program to respond to inquiries by federal, state and local government agencies seeking to verify or determine the citizenship or immigration status of any individual within the jurisdiction of the agency for any lawful purpose. See 8 U.S.C. § 1373(c). This authority allows agencies to use the Systematic Alien Verification for Entitlements Program for verification of citizenship and immigration status outside of the traditional benefit-granting programs covered by the Immigration Reform and Control Act of 1986. This includes voter registration and voter list maintenance purposes, so long as the agency meets the legal requirements for using the Systematic Alien Verification for Entitlements Program and provides the required applicant information, when submitting verification requests.

On January 20, 2025, and March 25, 2025, the President issued Executive Orders 14159, *Protecting the American People Against Invasion*¹² and 14248, *Preserving and Protecting the Integrity of American Elections*¹³ respectively. Executive Order 14159 requires the Secretary to “promptly issue guidance to ensure maximum compliance by [Department of Homeland Security] personnel with the provisions of 8 U.S.C. 1373¹⁴ and 8 U.S.C. 1644¹⁵ and ensure that State and local governments are provided with the information necessary to fulfill law enforcement, citizenship, or immigration status verification requirements authorized by law.” Executive Order 14248¹⁶ provides, “Federal laws, such as the National Voter Registration Act (Pub. L. 103-31) and the Help America Vote Act (Pub. L. 107-252), require States to maintain an accurate and current Statewide list of every legally registered voter in the State. Pursuant to the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Department of Homeland Security/United States Citizenship and Immigration Services is required to share database information with States upon request so they can fulfill this duty. 8 U.S.C. 1373(c)¹⁷.” Executive Order 14159¹⁸ directs the Secretary to “ensure that State and local officials have, without the requirement of the payment

¹² <https://www.federalregister.gov/documents/2025/01/29/2025-02006/protecting-the-american-people-against-invasion>

¹³ <https://www.federalregister.gov/documents/2025/03/28/2025-05523/preserving-and-protecting-the-integrity-of-american-elections>

¹⁴ 8 USC 1373 Communication between government agencies and the Immigration and Naturalization Service

¹⁵ 8 USC 1644 Communication between State and local government agencies and Immigration and Naturalization Service

¹⁶ Executive Order 14248 Preserving and Protecting the Integrity of American Elections

¹⁷ 8 USC. 1373(c) Obligation to respond to inquiries

¹⁸ Executive Order 14159 Protecting the American People Against Invasion



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 15 of 42

of a fee, access to appropriate systems for verifying the citizenship or immigration status of individuals registering to vote or who are already registered.” The Secretary is also required under Executive Order 14159, in coordination with the Department of Government Efficiency Administrator, to review each State’s publicly available voter registration list and available records concerning voter list maintenance activities as required by 52 U.S.C. 20507¹⁹, alongside Federal immigration databases and State records requested, including through subpoena where necessary and authorized by law, for consistency with Federal requirements. To support this activity the Attorney General is required to prioritize enforcement of 18 U.S.C. 611²⁰ and 1015(f)²¹ and similar laws that restrict aliens from registering to vote or voting, including through use of: (i) databases or information maintained by the Department of Homeland Security; (ii) State-issued identification records and driver license databases; and (iii) similar records relating to citizenship.

In accordance with federal statutes and policies, the Department of Homeland Security personnel must, in a timely manner, provide verification or immigration status information in response to inquiries from State and local government agencies to verify or ascertain the citizenship or immigration status of individuals. As required by 8 U.S.C. 1373(c), such inquiries must relate to individuals within the jurisdiction of the State or local government agency and must be for a purpose authorized by law. Department of Homeland Security personnel have been directed to comply, to the maximum extent possible and permissible under law, with Section 1373, considering federal statutory requirements, including the Privacy Act of 1974, 5 U.S.C. 552a²², and 8 U.S.C. 1367²³ (special protected class information); as well as other laws, rules, regulations, policies, and requirements regarding verification, information sharing, and confidentiality.

The Systematic Alien Verification for Entitlements Program user agency registration process determines whether a state voter registration agency meets the legal requirements for using the Systematic Alien Verification for Entitlements Program. As part of registering to use Systematic Alien Verification for Entitlements Program, the agency must provide the Systematic Alien Verification for Entitlements Program all applicable legal authorities and voter registration procedures that authorize the agency to engage in voter registration and/or voter list maintenance activities and verify citizenship status before making individual determinations regarding eligibility for voter registration. The United States Citizenship and Immigration Services provides information on its public facing website to assist user agencies understand the above referenced requirements.²⁴

Current Process - Voter Registration and Voter List Maintenance Verification

¹⁹ 52 USC 20507 Requirements with respect to administration of voter registration

²⁰ 18 USC 611 Voting by aliens

²¹ 18 USC 1015 (f) Naturalization, citizenship or alien registry, whoever knowingly makes any false statement or claims that he is a citizen of the United States in order to register to vote or to vote in any Federal, State, or local election (including an initiative, recall, or referendum)-Shall be fined under this title or imprisoned not more than five years, or both

²² 5 USC 552a Records maintained on individuals

²³ 8 USC 1367 Penalties for disclosure of information

²⁴ The Systematic Alien Verification for Entitlements Voter Registration and Voter List Maintenance Fact Sheet is accessible at <https://www.uscis.gov/save/resources/voter-registration-and-voter-list-maintenance-fact-sheet>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 16 of 42

In understanding the use of the Systematic Alien Verification for Entitlements Program for voter verification-related purposes (voter registration and voter list maintenance), one should also bear in mind the following limitations and considerations:

- The information needed to verify an individual through the Systematic Alien Verification for Entitlements Program is typically not collected on a voter registration application, although it may be available from other sources, especially driver's license applications.
- The Systematic Alien Verification for Entitlements Program previously was only able to verify United States citizenship for naturalized and certain acquired citizens²⁵ for whom the United States Citizenship and Immigration Services has a record of their citizenship.
- The Systematic Alien Verification for Entitlements Program previously was often unable to verify acquired United States citizens because eligible individuals frequently do not apply for and thus do not receive a determination and certificate of United States citizenship from the United States Citizenship and Immigration Services.
- Department of State adjudicates acquired citizens that may not have a record with the United States Citizenship and Immigration Services via the issuance of U.S. passports. Therefore, obtaining passport information from the Department of State is in progress.
- The Department of State maintains records for individuals who have renounced their citizenship. Once a Certificate of Loss of Nationality is approved by the Department of State indicating the official determination of loss of United States nationality, this information is shared with the United States Citizenship and Immigration Services per 8 USC 1373.²⁶
- With the newly established connection to the Social Security Administration's Numident system, the Systematic Alien Verification for Entitlements Program is now able to verify more United States citizens, including United States citizens by birth, when a Social Security Number is provided.

Verification for voter list maintenance purposes often occurs when a state Department of Motor Vehicles compares its records to the state voter agency records to determine if any individuals on the voter rolls identified that they were non-United States citizens when the Department of Motor Vehicles issued their driver's license. The state voter agency would then follow up with those individuals their citizenship status through established state law voter registration challenge procedures. As part of the established voter registration challenge procedures, the State Voter Agency will seek to establish the immigration/citizenship status of the individuals and use Systematic Alien Verification for Entitlements Program as one method to verify the information.

There are likely some situations in which the Systematic Alien Verification for Entitlements Program provides an initial response indicating a non-United States citizen immigration status (e.g., Lawful Permanent Resident) when the registrant is in fact a United States citizen. However, as also noted above, rules for using the Systematic Alien Verification for Entitlements Program prohibit voter registration agencies from relying upon this initial verification response to deny or revoke registration since as by

²⁵ "Acquired citizenship" refers to U.S. citizenship conveyed to children through the naturalization of parents or, under certain circumstances, at birth to foreign-born children of U.S. citizens, provided certain conditions are met.

²⁶ 8 USC 1873 outlines the communication between government agencies and the Immigration and Naturalization Service.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 17 of 42

asserting United States citizenship as part of registering to vote, registrants inherently disagree with any initial response indicating they are not a United States citizen.

Shortfalls in data accuracy in the system could cause incomplete or false results.

According to Systematic Alien Verification for Entitlements Program subject matter experts, the situations in which the Systematic Alien Verification for Entitlements Program provides an initial non-United States citizen immigration status for a United States citizen who has a certificate of naturalization or citizenship from the United States Citizenship and Immigration Services, or legacy Immigration and Naturalization Service can happen for a variety of reasons. In some instances, the initial non-United States citizen response is due to the lack of an electronic record with the Social Security Administration showing United States citizenship (which was not reliably recorded pre-1981), or the lack of an electronic record of a United States Citizenship and Immigration Services naturalization or acquired citizenship certificate, which is more likely for older certificates issued before recording them in electronic systems became a consistent practice. In addition, although the electronic record-matching algorithms in the United States Citizenship and Immigration Services Person Centric Service that the Systematic Alien Verification for Entitlements Program uses are very good, the United States Citizenship and Immigration Services previously identified and subsequently fixed two algorithm issues that caused Systematic Alien Verification for Entitlements Program to provide an initial verification response of Lawful Permanent Resident for some naturalized citizens and a small number of acquired United States citizens. But again, many of the safeguards noted above are designed to address any imperfections in records and algorithms used to match them.

The delay between the issuance a Certificate of Naturalization during a naturalization ceremony and when the certificate is reflected in source systems and made available to the Systematic Alien Verification for Entitlements Program rarely, if ever, causes the Systematic Alien Verification for Entitlements Program to provide an initial response of non-United States citizen immigration status. It typically takes about one business day plus a few hours for an electronic record of the certificate to be available to the Systematic Alien Verification for Entitlements Program once it is input by the responsible United States Citizenship and Immigration Services office. The Systematic Alien Verification for Entitlements Program rarely, if ever, receives requests to verify United States citizenship during this time.

Additionally, the United States Citizenship and Immigration Services is not the source agency for Social Security Administration related information. While the United States Citizenship and Immigration Services assumes the accuracy of the Social Security Administration data, it cannot verify accuracy of the information and relies on the Social Security Administration to ensure the data accuracy, timeliness, and integrity of their own data.

Customs and Border Protection Integration

The Systematic Alien Verification for Entitlements Program will integrate with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data. Customs and Border Protection is now permitting the Systematic Alien Verification for Entitlements Program to query TECS (not an acronym) Travel Documents and Encounter Data system to find a match to US passport information in Customs and Border Protection holdings. The TECS (not an acronym) - Travel Documents and Encounter Data system stores travel document information (i.e. scanned images of documents, biographic information, document details, and photographs) from the United States Citizenship and Immigration Services Lawful Permanent Resident Cards, Department of State-issued United States



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 18 of 42

passports and visas, foreign passports, enhanced driver's licenses, and enhanced tribal cards. The TECS (not an acronym) - Travel Documents and Encounter Data USPassportRESTService allows interconnected systems to query TECS (not an acronym) - Travel Documents and Encounter Data for United States passport information. For this use case, the Systematic Alien Verification for Entitlements Program user agencies will input a United States passport number into the Systematic Alien Verification for Entitlements Program system.

The query will trigger the USPassportRESTService to locate the matching United States passport number and return the results to the user. This will allow the Systematic Alien Verification for Entitlements Program to verify all types of United States citizens, including those by birth, which was previously not available. Currently, the United States Citizenship and Immigration Services E-Verify Program has an existing connection to the USPassportRESTService, which also resides within the Verification Information System, like the Systematic Alien Verification for Entitlements Program.

Customs and Border Protection has the authority to collect passport photos pursuant to 5 USC 552a (4).²⁷ Customs and Border Protection receives a routine feed from the Department of State with US passports as they are issued and/or updated. Customs and Border Protection also collects passport information primarily on all travelers seeking to enter the United States at ports of entry. Customs and Border Protection uses this information as part of Agency operations.

Social Security Administration Data Sharing

The Information Sharing Agreement between the Department of Homeland Security-United States Citizenship and Immigration Services and the Social Security Administration documents the Social Security Administration's support by matching data submitted through the Systematic Alien Verification for Entitlements Program to Social Security Administration records in the Social Security Administration's master files of Social Security Number holders and Social Security Number Applications. The United States Citizenship and Immigration Services will only submit verification requests to the Social Security Administration for authorized purposes.

The United States Citizenship and Immigration Services Verification Division and Social Security Administration connection is now live and now connects the Systematic Alien Verification for Entitlements Program with the Social Security Administration's Numident system. Prior to the connection, the United States Citizenship and Immigration Services and Social Security Administration executed a Letter of Agreement that identifies the authorities for both organizations as well as purposes and the data exchange. The United States Citizenship and Immigration Services will document this sharing in a separate Privacy Threshold Analysis.

The Systematic Alien Verification for Entitlements Program performs an automated query of various Systematic Alien Verification for Entitlements Program-accessed federal databases for relevant records. Now, if a Social Security Number is submitted by a user agency, the Systematic Alien Verification for Entitlements Program will verify this enumerator against the Social Security Administration Numident system including the death and citizenship records. If the individual's Social Security account has a record of an A-number or certificate number, the Social Security Administration will provide that information to the Systematic Alien Verification for Entitlements Program, which will in turn be used to

²⁷ 5 USC 552a (4) Records maintained on individuals - collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 19 of 42

validate the information against the Department of Homeland Security records. Verifying citizenship status using Social Security Administration data will be made available to all Systematic Alien Verification for Entitlements Program user agencies.

Department of State Data Sharing

If a United States passport number is submitted, the Systematic Alien Verification for Entitlements Program will verify it against information from Department of State-issued passports maintained by the Custom Boarder Protection. Additionally, Systematic Alien Verification for Entitlements Program will collect information from the Department of State’s Consular Consolidated Database / American Citizen Record Query system, which is a consular search engine used by the Department of State to manage and access records related to United States citizens, particularly for consular protection and services, including managing passport requests and applications.

Department of Homeland Security-Department of State Memorandum of Agreement Appendix A allows this query of passport information to be used in Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data to support its missions, including but not limited to verification of United States passports, whenever the document is presented as proof of identity to obtain a benefit, privilege, status, or credential from the Department of Homeland Security, for vetting and screening purposes, and/or for transportation security, national security, law enforcement, border security (including biometric entry and exit initiatives), immigration (including verification purposes such as E-Verify) and counterterrorism purposes.

User Agencies Memoranda of Agreement

All user agency memorandums of agreements contain similar provisions to protect the due process and other rights of individuals for whom states or other user agencies submit verification requests to the Systematic Alien Verification for Entitlements Program²⁸. The United States Citizenship and Immigration Services has an online tool that allows the public to search if a federal, state, local, tribal, or territorial agency is registered with the Systematic Alien Verification for Entitlement Program.²⁹

<p>2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> This project does not collect, collect, maintain, use, or disseminate any personally identifiable information³⁰</p> <p><input checked="" type="checkbox"/> Members of the public</p>
--	---

²⁸ The Systematic Alien Verification for Entitlements Program memorandum of agreement is assessable at <https://www.uscis.gov/save/prospective-user-agencies/register-an-agency-for-save> and under the “How to Register for SAVE” section.

²⁹ The Systematic Alien Verification for Entitlement Program search tool is accessible at <https://www.uscis.gov/save/save-agency-search-tool>.

³⁰ DHS defines personal information as “Personally Identifiable Information” or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. “Sensitive PII” is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 20 of 42

	<input checked="" type="checkbox"/> U.S. Persons (U.S citizens or lawful permanent residents) <input checked="" type="checkbox"/> non-U.S. Persons <input checked="" type="checkbox"/> DHS Employees/Contractors (list Components): United States Citizenship and Immigration Services <input type="checkbox"/> Other federal employees or contractors (list agencies): <i>Click here to enter text.</i>
<p>2(a) Is information meant to be collected from or about sensitive/protected populations?</p>	<input type="checkbox"/> No <input checked="" type="checkbox"/> 8 USC § 1367 protected individuals (e.g., T, U, VAWA) ³¹ <input checked="" type="checkbox"/> Refugees/Asylees <input type="checkbox"/> Other. Please list:
<p>3. What specific information about individuals is collected, maintained, used, or disseminated?</p>	
<p><u>Information Collected from Requesting Agencies about applicants for benefits, licenses, or other authorized purposes:</u></p> <ul style="list-style-type: none"> • Full Name • Date of birth • Benefit sought • Driver license • State Identification • Citizenship or nationality • Country of birth • A-Number • Social Security Number • Alias • Customer Agency-issued Case Number <p><u>Unique Immigration Identifiers Used:</u></p>	

³¹ This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at* <http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/002-02.pdf>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 21 of 42

- Alien number
- United States Citizenship and Immigration Services Number
- I-94 Admission Record Number (a 11-digit admission record assigned to foreign visitors entering the United States by the United States Customs and Border Protection)
- Student and Exchange Visitor Information System Identification Number
- Naturalization or Citizenship Certificate Number
- Card Number / I-797 Receipt Number (unique identifier assigned by the United States Citizenship and Immigration Services to track an immigration application or petition).
- Visa Number
- Foreign passport number (if submitted with another immigration enumerator and issuing country)

Other Identifiers:

- Social Security Number including a truncated version of the Social Security Number where only the last four digits are displayed, with the initial five digits are masked using asterisks (*) or XXXXX
- United States Passport Number
- Agency Data Universal Numbering System

Other Information:

Additional information requested by the agency:

- Employment Authorization Document History
- Grant Date
- Affidavit of Support Sponsor Data³²
 - Full name
 - Current mailing address - In care of name (if any)
 - Current physical address
 - Country of domicile
 - Date of birth
 - Country of birth
 - Social Security Number
 - Immigration Status
 - Sponsors A-number (if any)
 - United States Citizenship and Immigration Services Online Account Number (if any)
 - Military service
 - Employment and income
 - Federal tax return information

³² A United States Citizenship and Immigration Services Affidavit of Support sponsor is an individual who signs a legal contract, Form I-864, agreeing to financially support an intending immigrant, ensuring they won't become a public charge. This sponsor is typically the U.S. citizen, lawful permanent resident, or U.S. national who filed the immigrant petition.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 22 of 42

- Sponsor Deeming and Agency Reimbursement Information Collection
 - Whether the benefit-granting agency approved or denied the application for the means-tested public benefit.
 - If the benefit-granting agency denied the application, if the denial was based upon the information that the Systematic Alien Verification for Entitlements Program provided in its response to the citizenship and immigration status verification request from the benefit-granting agency.
 - Whether the benefit-granting agency deemed sponsor/household member income and, if not, the exception or reason for not doing so.
 - Whether the benefit-granting agency sent the sponsor a reimbursement request letter (yes/no).
 - Whether the sponsor complied with his or her reimbursement obligation.
 - Whether the benefit-granting agency conducted a collection action or other proceedings if the sponsor did not comply with his or her reimbursement obligation (yes/no and if yes, the status, court or forum, and docket or matter number).
- Data collected on Form I-864, Affidavit of Support Under Section 213A of the Immigration and Nationality Act
 - Principal Immigrant:
 - Full name
 - Current mailing address - In care of name (if any)
 - Current physical address
 - Country of Citizenship or Nationality
 - Date of birth
 - Alien Registration number
 - United States Citizenship and Immigration Services Online Account Number (if any)
 - Daytime telephone number
 - Principal Immigrant Family Members:
 - Full name
 - Relationship to Principal Immigrant
 - Alien Registration number
 - United States Citizenship and Immigration Services Online Account Number (if any)
 - Daytime telephone number
 - Interpreter's Contact Information, Certification and Signature:
 - Full name
 - Telephone number
 - Email address (if any)
 - Interpreter's certification and signature
 - Preparer's Contact Information:
 - Daytime number
 - Mobile number (if any)
 - Email address (if any)
 - Signature
- Cuban/Haitian, Immigration Status



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 23 of 42

- Violence Against Women's Act
- Request Document Review
- Citizenship Status
- Immigration Documentation (uploaded by the user agency to perform additional verification)

Agency User Information

- Agency point of contact name
- Agency point of contact phone number
- Initiated on
- Initiated by

Information Shared with Social Security Administration:

- Full Name
- Date of Birth
- Social Security Number

DATA Received and Maintained from Social Security Administration:

- Social Security Number Match: True/False
- Name Match: True/False
- Date of Birth Match: True/False
- Citizenship Indicator:
 - "A" - United States citizen
 - "B" - Legal alien, eligible to work
 - "C" - Legal alien, not eligible to work
 - "D" - Other
 - "E" - Alien Student - restricted work authorized
 - "F" - Conditionally legalized alien
- Foreign Born Indicator: Citizenship code is not present, but individual was foreign born
- Alien Registration Number: Where applicable
- Certificate Number: Where applicable
- Death Indicator: Yes Deceased / Not Deceased
- Error Code Descriptions: Transaction and record levels

Information Shared with TECS (not an acronym) – TECS (not an acronym)-Travel Documents and Encounter Data for Passport query:

- Full Name
- Date of Birth
- United States passport number



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 24 of 42

Information Provided to Requesting User Agencies:

- Case Verification Number: a Systematic Alien Verification for Entitlements Program generated number
- Initial Request Date
- Identification Type
- Identification Number
- Last Name
- Benefit Code
- Benefit Description
- Initial Request Response: Lawful Status, No Lawful Status, Deceased
- Additional Request Date
- Additional Request Response: Lawful Status, No Lawful Status, Deceased
- Third Step Request Date
- Third Step Resolution: Lawful Status, No Lawful Status, Deceased

Additional information for immigrants requested from agencies for which they established the authority/need to receive

- Employment authorization document history
- Grant date
- Affidavit of Support Sponsor Data
- Cuban/Haitian Entrant Information
- Violence Against Women’s Act information
- Immigration Status
- Request document review
- Citizenship status
- Photo
- Closed Date
- Receipt number

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?³³ If applicable, check all that apply.

³³ Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, available at <https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information>.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 25 of 42

<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Social Security number <input checked="" type="checkbox"/> Alien Number (A-Number) <input type="checkbox"/> Tax Identification Number <input checked="" type="checkbox"/> Visa Number <input checked="" type="checkbox"/> Passport Number <input type="checkbox"/> Bank Account, Credit Card, or other financial account numbers 	<ul style="list-style-type: none"> <input type="checkbox"/> Social Media Handle/ID <input checked="" type="checkbox"/> Driver's License/State ID Number <input type="checkbox"/> Biometric identifiers (e.g., <i>FIN, EID</i>) <input checked="" type="checkbox"/> Biometrics.³⁴ <i>Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.</i> <input checked="" type="checkbox"/> Other. <i>Please list:</i> Form I-94 number, Student and Exchange Visitor Information System Identification number, Naturalization / Citizenship Certificate number, Permanent Resident Card number / Receipt number, and Visa number.
<p>3(b) Please provide the specific legal basis for the collection of SSN:</p>	<p>The Social Security Number is collected from applicants and is used to verify their immigration status/United States citizenship. div. C, title VI, Section 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-707, codified at 8 U.S.C. 1373 (a) and (c). Authority for having a system for verification of citizenship and immigration status of individuals seeking government benefits is governed by the Immigration Reform and Control Act of 1986 Pub. L. No. 99-603, 100 Stat. 3359.</p> <p>Sections 415 and 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, authorizes the collection and use of Social Security Numbers to verify entitlement to public benefits, licenses, and credentials.</p>
<p>3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.</p>	
<p>The Social Security Number is used to assist in identity verification for user agencies and in determining benefits eligibility. If possible, the United States Citizenship and Immigration Services will use a truncated Social Security Number if provided by the user agency.</p>	

³⁴ If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 26 of 42

3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,³⁵ which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: *even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.*

The United States Citizenship and Immigration Services has traditionally used an alternative number to the Social Security Number to access records to determine the citizenship/immigration status of user agencies benefit applicants in compliance with the Department of Homeland Security privacy-related policies. However, United States Citizenship and Immigration Services now needs to collect Social Security numbers to facilitate user agencies' ability to submit a request for citizenship/immigrations status of benefit applicants. The United States Citizenship and Immigration Services is working to implement use of the truncated form of a Social Security number (i.e. the last four numbers of a Social Security number rather than the full identifier) to retrieve information from the Social Security Administration. The Systematic Alien Verification for Entitlements Program's user interface will mask the full Social Security Number during data inputs, except for when information is submitted via the bulk uploader. In compliance with the security policy for Social Security numbers, server-side encryption is used for Amazon Simple Storage Service³⁶ and Amazon Relational Database Services³⁷ databases. This uses key management provided by Amazon Web Services for the storage buckets and Relational Database Services databases where Social Security Numbers are housed. Social Security Numbers and Personally Identifiable Information are not exposed in any hard copy documents available for extract from the information system. Additionally, in accordance with the National Institute of Science and Technology and Department of Homeland Security information security and privacy policies, the Systematic Alien Verification for Entitlements Program maintains moderate level controls for the confidentiality of information within the tool.

<p>4. How does the Project, Program, or System retrieve information?</p>	<p><input checked="" type="checkbox"/> By a unique identifier.³⁸ Please list all unique identifiers used:</p> <ul style="list-style-type: none"> • Full name • Alias
---	---

³⁵ See <https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction>.

³⁶ Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. Organizations can use this service to store, manage, analyze, and protect any amount of data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps.

³⁷ Amazon Relational Database Service (Amazon RDS) is an easy-to-manage relational database service optimized for total cost of ownership. It is simple to set up, operate, and scale with demand. Amazon RDS automates undifferentiated database management tasks, such as provisioning, configuring, backing up, and patching. Amazon RDS allows customers to create a new database in minutes and offers flexibility to customize databases to meet their needs.

³⁸ Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 27 of 42

	<ul style="list-style-type: none"> • Date of birth • Immigration enumerator: <ul style="list-style-type: none"> ○ Alien number/United States Citizenship and Immigration Services Number, ○ Form I-94, Arrival/Departure Record number, ○ Student and Exchange Visitor Information System Identification number, ○ Citizenship or Naturalization Certificate number ○ Card Number / I-797 Receipt Number, ○ Visa Number, or ○ Foreign passport number (if submitted with another immigration enumerator) and issuing country • Social Security Number • United States passport number • Customer Agency-issued Case Number • Case Verification Number <p><input type="checkbox"/> By a non-unique identifier or other means. Please describe: <i>Click here to enter text.</i></p>
--	---

<p>5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? If no schedule has been approved, please provide proposed schedule or plans to determine it.</p> <p><i>Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.³⁹</i></p>	<p>Data within Systematic Alien Verification for Entitlements Program is retained for 10 years after the final match determination of the employee or applicant in accordance with NARA approved records retention schedule N1-566-08-07.</p> <p>All United States Citizenship and Immigration Services verification requests will be documented in a transactional database. The retention period is 10 years. The database is not accessible to the public, except as permitted.</p>
--	--

³⁹ See <https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/cdod/rm/Pages/DHS-Records-Officers.aspx>



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 28 of 42

<p>5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)?</p>	<p>Data is automatically purged annually based on NARA disposal schedule NI-566-08-07.</p>
<p>6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?⁴⁰</p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>United States Citizenship and Immigration Services Systems:</p> <ul style="list-style-type: none"> • Central Index System • Electronic Immigration System • Computer Linked Application Information Management System 3 • Enterprise Citizenship and Immigration Services Centralized Operational Repository • GLOBAL (not an acronym) • RAILS (not an acronym) • Customer Profile Management System • Reengineered Naturalization Application Casework System • Marriage Fraud Amendment System • Salesforce Customer Relationship Management Customer Relationship Management⁴¹ <p>Department of Homeland Security Systems:</p> <ul style="list-style-type: none"> • Department of Homeland Security OneNet • Immigration and Custom Enforcement Student and Exchange Visitor Information System • Immigration and Custom ENFORCE Integrated Database

⁴⁰ PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes.

⁴¹ Provides a unified platform where data from different departments can be accessed and used to improve customer interactions.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 29 of 42

	<ul style="list-style-type: none"> • Customs and Border Protection Arrival and Departure Information System • Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data - USPassportRESTService • Transportation Security Administration Technology Infrastructure Modernization and Vetting and Credentialing System
<p>7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?</p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>The following are systems/organizations that the Systematic Alien Verification for Entitlements Program collects/shares information to support user agencies' requests:</p> <ul style="list-style-type: none"> • United States Military Entrance Processing Command Integrated Resource System • Department of Education Federal Student Aid Central Processing System • Department of Health and Human Services Centers for Medicare & Medicaid Services • Social Security Administration Numident system • Department of Justice Executive Office for Immigration's Immigration Review Information Exchange System • Department of State Consular Consolidated Database Passport <p>The following are systems/organizations that the Systematic Alien Verification for Entitlements provides information that determine benefit eligibility:</p> <ul style="list-style-type: none"> • Various federal agencies in their role as a user agency



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 30 of 42

	<ul style="list-style-type: none"> • Various state, local, tribal, and territory agencies in their role as a Systematic Alien Verification for Entitlements Program user agency
<p>8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? If applicable, please provide agreement as an attachment.</p>	<p>Existing</p> <p>Please describe applicable information sharing governance in place:</p> <ul style="list-style-type: none"> • Letter of Agreement between United States Citizenship and Immigration Services and Social Security Administration • Information Sharing Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services and the Social Security Administration regarding citizenship • Computer Matching Agreement with Department of Education • Memorandum of Agreements between United States Citizenship and Immigration Services and each individual user agency
<p>9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?</p>	<p><input type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: <i>Click here to enter text.</i></p> <p><input checked="" type="checkbox"/> Yes. In what format is the accounting maintained if appropriate (e.g., disclosures to the Department of Justice Office of Special Counsel, Immigration and Customs Enforcement). Verification Information System also has a transactional log that enables the recreation of accounting of disclosures.</p>
<p>10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:</p>	<p><input type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Advanced analytics⁴²</p> <p><input type="checkbox"/> Live PII data for testing</p>

⁴² The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 31 of 42

	<input checked="" type="checkbox"/> No
11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?⁴³ This does not include subject-based searches.	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i>
11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i>
12. Does the planned effort include any interaction or intervention with human subjects⁴⁴ via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for <u>independent</u> review and approval of this effort. ⁴⁵
13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, <u>in addition</u> to annual privacy training required of all DHS personnel?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: <i>Click here to enter text.</i>

⁴³ Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—
 (A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals.
 (B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
 (C) the purpose of the queries, searches, or other analyses is not solely—
 (i) the detection of fraud, waste, or abuse in a government agency or program; or
 (ii) the security of a government computer system.

⁴⁴ Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

⁴⁵ For more information about CAPO and their points of contact, please see: <https://www.dhs.gov/publication/capo> or <https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36>. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
 Page 32 of 42

<p>14. Is there a FIPS 199 determination?⁴⁶</p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following:</p> <p>Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Integrity: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Availability: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p>
---	--

PTA REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE REVIEWER)

Component Privacy Office Reviewer:	Chiquita Jones/LeVar Sykes
Component Privacy Office Senior Reviewer:	Shannon DiMartino
PRIVCATS ID Number:	0019946
Date submitted to Component Privacy Office:	May 5, 2025
Concurrence from other Component Reviewers involved (if applicable):	Catherine Shorten, Customs and Border Protection, concurrence provided 6/5/2025
<p>Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.</i></p> <p>The United States Citizenship and Immigration Services submits this updated Privacy Threshold Analysis to document the United States Citizenship and Immigration Services Verification Division and Office of Technology (OIT) changes to the Systematic Alien Verification for Entitlements Program. The United States Citizenship and Immigration Services administers the Systematic Alien Verification for Entitlements Program which is an inter-governmental initiative that provides a web-based service to help</p>	

⁴⁶ FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems. For more information, see <https://www.nist.gov/itl/fips-general-information>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 33 of 42

federal, state, territorial, tribal and local agencies and other governmental entities verify United States citizenship or immigration status/category information of applicants for benefits, licenses, or other authorized purposes.

This Privacy Threshold Analysis documents the following changes to the Systematic Alien Verification for Entitlements Program:

1. Expanded search capabilities to allow approved Systematic Alien Verification for Entitlements Program user agencies to verify United States citizenship information using Social Security Numbers and other non-Department of Homeland Security enumerators.
2. A new Social Security Administration system connection to support verification of citizenship/immigration status.
3. A new bulk uploader/list processor function that allows user agencies to upload lists of benefit applicants.
4. Use of the Voter Registration and Voter List Maintenance Verification functionality.
5. The collection of information from the Department of State's Consular Consolidated Database/American Citizen Record Query system.
6. An integration with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data system.

The United States Citizenship and Immigration Services Privacy Office recommends Privacy Impact Assessment coverage for the Systematic Alien Verification for Entitlements Program to comply with the eGovernment Act of 2002 as it "collects, maintains, or disseminates information that is in an identifiable form." The information collected, used, stored, and/or disseminated by the Systematic Alien Verification for Entitlements Program meets the definition of Personally Identifiable Information ("PII")/Sensitive Personally Identifiable Information ("SPII")⁴⁷ as it "permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether that individual is a United States citizen, legal permanent resident, or a visitor to the United States, or employee or contractor to the Department." Specifically, the Systematic Alien Verification for Entitlements Program involves information from members of the public applying for benefits, licenses, or other authorized purposes which may include (1) United States citizens and legal permanent residents, (2) individuals who are now current United States citizens and legal permanent residents after previously naturalizing or adjusting their status, or (3) individuals who may ultimately naturalize to become United States citizens or adjust their status to receive legal permanent residency in the future. Depending on the eligibility category certain individuals may be eligible to apply for adjustment of status as soon as one (1) year after their initial immigration benefit is granted,⁴⁸ therefore the United States Citizenship and Immigration Services Privacy Office recommends requiring Privacy Impact Assessment coverage for the Systematic Alien Verification for Entitlements Program to ensure all current and future United States

⁴⁷ Personally Identifiable Information (PII) has numerous official definitions, but in general, it is defined as any information that can be used to identify an individual directly or indirectly, such as a name, email address, Social Security Number or IP address. Sensitive PII (SPII) is generally defined as any PII that if lost, stolen, or disclosed without authorization could result in significant harm to an individual.

⁴⁸ For more information on eligibility categories please refer to: <https://www.uscis.gov/green-card/green-card-eligibility-categories>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 34 of 42

citizens and legal permanent residents have transparency into how the United States Citizenship and Immigration Services may collect, store, use, and share the information they previously provided to the United States Citizenship and Immigration Services.

The Privacy Office's Technology Oversight Branch recommends that the Systematic Alien Verification for Entitlements Program continues to be designated as a privacy sensitive program that requires privacy compliance coverage. The Technology Oversight Branch recommends that with the new updates to the program documented in this Privacy Threshold Analysis the Systematic Alien Verification for Entitlements Program be identified as not in compliance with the Privacy Act of 1974, as amended, or the E-Government Act of 2002. A Privacy Impact Assessment update and a System of Records Notice update should be published prior to the program's changed collection and use of Personally Identifiable Information, including information on natural born United States citizens. Further, the sharing of Personally Identifiable Information with the Social Security Administration should occur after the System of Records Notice has gone through the required 30-day comment period. The following are the Technology Oversight Branch's recommendations for privacy compliance coverage and additional requirements:

Privacy Impact Assessment

- A new Privacy Impact Assessment Update for DHS/USCIS/PIA-006 Systematic Alien Verification for Entitlements Program must be completed before collection and use of additional information. Specifically, these Privacy Impact Assessment updates would include, but are not limited to:
 - The collection of Social Security Numbers and other information from the Social Security Administration regarding United States citizens, including natural born citizens.
 - The change in legal rationale for now collecting and maintaining Social Security Numbers of United States natural born citizens.
 - The collection and use of Passport Numbers from the Department of State via new system connections.
 - The addition of the Voter Registration and Voter List Maintenance Verification process, including how this process may verify the citizenship status of natural born United States citizens.
 - The implementation of the bulk case upload functionality for User Agencies.
 - Additional privacy risks and mitigation strategies regarding notice, consent, and data accuracy.

System of Records Notice

- An update to DHS/USCIS-004 Systematic Alien Verification for Entitlements Program must be completed before the collection and sharing of additional information. Specifically, these System of Records Notice updates would include, but are not limited to changes to the following sections:
 - Purpose: The System of Records Notice does not currently include the verification of voter registration and voter maintenance lists.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 35 of 42

- Categories of Individuals: Currently, USCIS specifically informs the public it only collects information on naturalized or acquired United States citizens. This section must be updated to discuss that information on natural born United States citizens will also be collected.
- Categories of Records: The System of Records Notice currently informs the public that the Systematic Alien Verification for Entitlements Program only collects Social Security Number of immigrants on the United States Citizenship and Immigration Services Form G-845. This section must be updated to cover the expanded collection and use of Social Security Numbers.
- Sources of Records: The System of Records Notice currently doesn't include the Social Security Administration system of records. This section must be updated to reflect all new source systems including the Social Security Administration Numident system.
- DHS/CBP-011 Customs and Border Protection Primary and Secondary Processing (TECS (not an acronym)) National SAR Initiative December 19, 2008 (73 Federal Register 77778)
- STATE-26 Passport Records, March 24, 2015 (80 Federal Register 15653)
- STATE-39 Visa Records, November 8, 2021 (86 Federal Register 61822)
- SSA-60-0058 Master Files of Social Security Number Holders and Social Security Number Applications, February 20, 2025 (90 Federal Register 10025)

The following is a Plan of Action to ensure that the Systematic Alien Verification for Entitlements Program is brought into compliance with all federal statutes, regulations, and Department of Homeland Security policies.

USCIS Privacy's Action Plan for the Systematic Alien Verification for Entitlements Program

The Systematic Alien Verification for Entitlements Program is an inter-governmental initiative that provides a web-based service to help federal, state, territorial, tribal and local agencies and other governmental entities verify United States citizenship or immigration status/category information of applicants for benefits, licenses, or other authorized purposes.

Action Plan

This plan outlines priority actions necessary to advance the goal and objective of ensuring the Systematic Alien Verification for Entitlements Program is compliant with all applicable privacy laws, regulations, and policies. These actions will ensure that the use of technology by United States Citizenship and Immigration Services and the Systematic Alien Verification for Entitlements Program sustains and does not erode privacy protections relating to the collection, use, dissemination, maintenance, and disposal of personal information. These actions include actively working with the Verification Division, Office of Chief Counsel and the Customs and Border Protection Office of Privacy on this Privacy Threshold Analysis and the draft System of Records Notice along with continued collaboration with these stakeholders and others such as the Department of Homeland Security Privacy Office to ensure Systematic Alien Verification for Entitlements Program is in compliance.

Actions to Be Taken



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 36 of 42

To meet these objectives the United States Citizenship and Immigration Services Office of Privacy will complete the following activities:

- Receive United States Citizenship and Immigration Services Chief Privacy Officer adjudication of the initial Systematic Alien Verification for Entitlements Program Privacy Threshold Analysis:
 - Adjudication - Estimated Date of Completion: July 2025
- Draft an updated Systematic Alien Verification for Entitlement Program Privacy Impact Assessment meeting all requirements identified above and submit the draft to the Department of Homeland Security Office of Privacy.
 - Initial Draft - Estimated Date of Completion: July 2025
 - Office of Chief Counsel Review – Estimated Date of Completion: July 2025
 - Submission to Department of Homeland Security – Estimated Date of Completion: August 2025
 - Publication – Estimated August 2025
- Draft an updated Systematic Alien Verification for Entitlement Program System of Records Notice meeting all requirements identified above and submit the draft to the Department of Homeland Security Office of Privacy.
 - Initial Draft - Estimated Date of Completion: June 2025
 - Office of Chief Counsel Review – Estimated Date of Completion: June 2025
 - Submission to Department of Homeland Security – Estimated Date of Completion: July 2025
 - Submission to the Office of Management and Budget and Congress – Estimated July 2025
 - Publication – Estimated July 2025
 - End of 30-day commenting period (and sharing of new routine uses) Estimated August/September 2025
- Draft a Privacy Threshold Analysis documenting the new Systematic Alien Verification for Entitlement Program information sharing agreement between the United States Citizenship and Immigration Services and the Social Security Administration and receive the Chief Privacy Officer's adjudication of the Privacy Threshold Analysis.
 - Estimated Date of Completion: July 2025
- Determine the applicability of the Computer Matching and Privacy Protection Act of 1988 to new or changed aspects of the Systematic Alien Verification for Entitlements Program including the new bulk upload functionality for User Agencies.
 - Hold a discussion regarding the Computer Matching Agreement impacts with representatives from the Department of Homeland Security Privacy Office, United States



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 37 of 42

Citizenship and Immigration Services Office of Chief Counsel and Office of Privacy, and Department of Homeland Security Office of General Council.

- Date of Completion: June 2025
- Decide on the need for Computer Matching Agreements with user agencies versus the current Memorandum of Agreements in place with each Systematic Alien Verification for Entitlement Program user agency:
 - Estimated Date of Completion: July 2025

This Privacy Threshold Analysis and Action Plan focuses predominantly on Phases One through Four of the Systematic Alien Verification for Entitlements Program Optimization effort as Phase Five and Phase Six are longer term goals of the optimization effort and are still in the exploratory/planning stage. The United States Citizenship and Immigration Services will update this Privacy Threshold Analysis and Action Plan as needed to support the remaining phases during their development and ensure the Systematic Alien Verification for Entitlements Program is compliant with all applicable laws, regulations, and Department of Homeland Security policies.

The updated Privacy Threshold Analyst should also provide, at a minimum, the following updates:

- New status types that Systematic Alien Verification for Entitlements Program may provide to the user agencies and how any additional verification is completed.
- A discussion about the update to the user memorandum of agreements and the creation of the voter verification specific memorandum of agreements.
- Confirm all responses from the Customs and Border Protection via the use of their USPassportRESTService when matching United States Passport numbers.
- Discuss Customs and Border Protection authority/purpose for collecting United States Passport related photographs and collection of those photographs by the United States Citizenship and Immigration Services.
- A description of how the information received via the integration with the Department of Justice to enable an incarceration/felony related flag will be used internally and if any related information will be sent to the user agencies or the applicants.
- If the Systematic Alien Verification for Entitlements Program will use the existing connection by the E-Verify Program to the USPassportRESTService or will it be a new connection.
- Additional use case information for the Systematic Alien Verification for Entitlements Program use of Department of State information from the USPassportRESTService and the Department of State's Consular Consolidated Database / American Citizen Record Query system.
- Clarification regarding user agency benefit applicants accessing the Systematic Alien Verification for Entitlements Program.
- Additional information regarding notification provided to United States citizens regarding user agencies use of their information.
- What information may be provided to the user agency about the VAWA status of an individual.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 38 of 42

- Discussion of if there could be instances when a natural born United States citizen is unable to be verified based on the data available. Also, if all United States citizens would be able to be verified via the SSA information.
- Confirmation if there are additional responses (besides Lawful Status, No Lawful Status, or Deceased) provided to user agencies now that United States citizens can also be verified.
- A discussion of any updates regarding any new agreements between Department of State and Customs and Border Protection for the sharing and use of United States Passport number information.
- Confirmation of if there is still a connection with the Reengineered Naturalization Application Casework System (which was previously decommissioned) or how information from the previously decommissioned system is still accessed.

PTA ADJUDICATION

(TO BE COMPLETED BY THE COMPONENT PRIVACY OFFICE APPROVER)

Component Privacy Office Approver:	Angela Y. Washington
PTA Approval Date:	July 17, 2025
PTA Expiration Date:	October 17, 2025

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	System If "other" is selected, please describe: <i>Click here to enter text.</i>
Determination:	<input type="checkbox"/> Project, Program, System in compliance with full coverage. <input type="checkbox"/> Project, Program, System in compliance with interim coverage. <input type="checkbox"/> Project, Program, System in compliance until changes implemented. <input checked="" type="checkbox"/> Project, Program, System not in compliance.
PIA:	PIA Update is required. <ul style="list-style-type: none"> • DHS/USCIS/PIA-006 Systematic Alien Verification for Entitlement Program <ul style="list-style-type: none"> ○ This PIA must be updated to document all identified system/programmatic changes.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 39 of 42

SORN:	<p>SORN update is required.</p> <ul style="list-style-type: none"> • DHS/USCIS-004 Systematic Alien Verification for Entitlements Program, May 27, 2020 (85 FR 31798) <ul style="list-style-type: none"> ○ This SORN must be updated to document all identified changes. • DHS/CBP-011 Customs and Border Protection Primary and Secondary Processing (TECS (not an acronym)) National SAR Initiative December 19, 2008 (73 Federal Register 77778) • STATE-26 Passport Records, March 24, 2015 (80 Federal Register 15653) • STATE-39 Visa Records, November 8, 2021 (86 Federal Register 61822) • SSA-60-0058 Master Files of Social Security Number Holders and Social Security Number Applications, February 20, 2025 (90 Federal Register 10025)
<p>Component Privacy Office Adjudication: <i>Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.</i></p>	
<p>The USCIS Office of Privacy is submitting this Privacy Threshold Analysis (PTA) to document the Systematic Alien Verification for Entitlements (SAVE) Program. The Systematic Alien Verification for Entitlements Program is an intergovernmental initiative using a web-based service to help federal, state, territorial, tribal and local benefit-issuing and licensing agencies and other governmental entities determine the immigration status or United States citizenship of applicants for public benefits, licenses, grants, credentials, background investigations, and other lawful purposes, so only entitled applicants receive them. The Systematic Alien Verification for Entitlements Program verifies immigration status/category and United States citizenship against Department of Homeland Security-accessed records. The Systematic Alien Verification for Entitlements Program is not a database but queries Department of Homeland Security-accessed federal records to provide registered user agencies with a verification response. The Systematic Alien Verification for Entitlements Program does not determine an applicant’s eligibility for a specific benefit or license, as this is the responsibility of the benefit/license granting agency.</p> <p>This Privacy Threshold Analysis is being submitted to document multiple updates and planned updates to the Systematic Alien Verification for Entitlements Program as part of the comprehensive optimization of the Systematic Alien Verification for Entitlements Program to ensure a single, reliable source for verifying immigration status and United States citizenship nationwide. This Privacy Threshold Analysis documents the following key changes: (1) an expanded search capabilities to allow approved Systematic Alien Verification for Entitlements Program user agencies to verify United States citizenship information using Social Security Numbers and other non-Department of Homeland Security enumerators, (2) a new Social Security Administration system connection to support verification of citizenship/immigration status, (3) a new bulk uploader/list processor function that allows user agencies to upload lists of benefit applicants, (4) the use of the Voter Registration and Voter List Maintenance Verification functionality, (5) the collection of information from the Department of State’s Consular Consolidated Database/ American</p>	



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 40 of 42

Citizen Record Query system, and (6) an integration with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data system.

After a thorough review of the PTA, the USCIS Office of Privacy continues to designate the Systematic Alien Verification for Entitlements Program as a privacy sensitive system/program requiring both Privacy Impact Assessment (PIA) and System of Records Notice (SORN) coverage as it collects/uses Personally Identifiable Information (PII) as well as Sensitive Personally Identifiable Information (SPII) from members of the public, including legal permanent residents and United States Citizens.

The United States Citizenship and Immigration Services Office of Privacy recommends Privacy Impact Assessment coverage for the Systematic Alien Verification for Entitlements Program to comply with the eGovernment Act of 2002 as it “collects, maintains, or disseminates information that is in an identifiable form.” The information collected, used, stored, and/or disseminated by the Systematic Alien Verification for Entitlements Program meets the definition of Personally Identifiable Information (“PII”)/Sensitive Personally Identifiable Information (“SPII”)⁴⁹ as it “permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether that individual is a United States citizen, legal permanent resident, or a visitor to the United States, or employee or contractor to the Department.” Specifically, the Systematic Alien Verification for Entitlements Program involves information from members of the public applying for benefits, licenses, or other authorized purposes which may include (1) United States citizens and legal permanent residents, (2) individuals who are now current United States citizens and legal permanent residents after previously naturalizing or adjusting their status, or (3) individuals who may ultimately naturalize to become United States citizens or adjust their status to receive legal permanent residency in the future. Depending on the eligibility category certain individuals may be eligible to apply for adjustment of status as soon as one (1) year after their initial immigration benefit is granted,⁵⁰ therefore the United States Citizenship and Immigration Services Office of Privacy recommends requiring Privacy Impact Assessment coverage for the Systematic Alien Verification for Entitlements Program to ensure all current and future United States citizens and legal permanent residents have transparency into how the United States Citizenship and Immigration Services may collect, store, use, and share the information they previously provided to the United States Citizenship and Immigration Services.

Privacy Impact Assessment (PIA) coverage is provided by the following:

- DHS/USCIS/PIA-006 Systematic Alien Verification for Entitlement Program
 - **For the Systematic Alien Verification for Entitlement Program to be in compliance with the eGovernment Act of 2002, this Privacy Impact Assessment must be**

⁴⁹ Personally Identifiable Information (PII) has numerous official definitions, but in general, it is defined as any information that can be used to identify an individual directly or indirectly, such as a name, email address, Social Security Number or IP address. Sensitive PII (SPII) is generally defined as any PII that if lost, stolen, or disclosed without authorization could result in significant harm to an individual.

⁵⁰ For more information on eligibility categories please refer to: <https://www.uscis.gov/green-card/green-card-eligibility-categories>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 41 of 42

updated to reflect the identified system and programmatic changes along with a privacy risk assessment of these changes including but not limited to new collections of data, new populations impacted including natural born US citizens, new system connections, new data sharing, and a new bulk upload/reporting functionality.

System of Records Notice (SORN) coverage is required as the information in the Systematic Alien Verification for Entitlement Program is retrieved by a personal identifier. System of Records Notice coverage is provided by the following:

- DHS/USCIS-004 Systematic Alien Verification for Entitlements Program, May 27, 2020 (85 FR 31798)
 - **For the Systematic Alien Verification for Entitlement Program to be in compliance with the Privacy Act of 1974, this System of Records Notice must be updated to reflect the identified system and programmatic changes including that the System of Records will now include information on natural born United States citizens in addition to naturalized or acquired United States citizens. Updates to the System of Records Notice should include but are not limited to updates in the Purpose, Categories of Individuals, Categories of Records, and the Sources of Records sections.**
- DHS/CBP-011 Customs and Border Protection Primary and Secondary Processing (TECS (not an acronym)) National SAR Initiative December 19, 2008 (73 Federal Register 77778)
- STATE-26 Passport Records, March 24, 2015 (80 Federal Register 15653)
- STATE-39 Visa Records, November 8, 2021 (86 Federal Register 61822)
- SSA-60-0058 Master Files of Social Security Number Holders and Social Security Number Applications, February 20, 2025 (90 Federal Register 10025)

While there are currently published SORNs and PIAs associated with the Systematic Alien Verification for Entitlement Program, these documents do not sufficiently provide coverage for the recently implemented and planned system and programmatic changes documented in this Privacy Threshold Analysis. Therefore, the Systematic Alien Verification for Entitlement Program is not in compliance. An updated Privacy Impact Assessment and an updated System of Records Notice must be published for the Systematic Alien Verification for Entitlement Program to be brought into compliance.

An action plan has been developed to enable the Systematic Alien Verification for Entitlement Program to be brought into compliance with all federal laws, statutes, regulations, and Department of Homeland Security policies. A high-level summary of the action plan is as follows:

- Complete the initial Systematic Alien Verification for Entitlements Program Privacy Threshold Analysis.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 42 of 42

- Publish an updated Systematic Alien Verification for Entitlement Program Privacy Impact Assessment to the Department of Homeland Security Office of Privacy website.
- Publish an updated Systematic Alien Verification for Entitlement Program System of Records Notice in the Federal Register and address any comments received during the 30-day public comment period.
- Complete a Privacy Threshold Analysis documenting the new Systematic Alien Verification for Entitlement Program information sharing agreement between the United States Citizenship and Immigration Services and the Social Security Administration.
- Determine the applicability of the Computer Matching and Privacy Protection Act of 1988 and complete any identified requirements.
- Update the Systematic Alien Verification for Entitlements Program Privacy Threshold Analysis and Action Plan as needed to support the ongoing optimization effort.

The Office of Privacy approves this Privacy Threshold Analysis for 3 months to formally document the current privacy posture of the Systematic Alien Verification for Entitlement Program.

Exhibit 15



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 1 of 42

PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals, and to assess whether there is a need for additional privacy compliance documentation or requirements. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used. In accordance with the Fair Information Practice Principles (FIPPs),¹ Component Privacy Officers should consider best practices for privacy safeguards and principles when reviewing and adjudicating PTAs.

Please complete the attached PTA and submit it to your Component Privacy Office. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]

The Component or DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If privacy compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement/Privacy Notice, or Computer Matching Agreement (CMA) – the Component Privacy Office will send you a copy of the relevant compliance template to complete and return.

¹ See [The Fair Information Practice Principles | Homeland Security](#).



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 2 of 42

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	Systematic Alien Verification for Entitlements Program		
Component or Office:	U.S. Citizenship and Immigration Services (USCIS)	Office or Program:	Verification Division
FISMA Name (if applicable):	Verification Information System	FISMA Number (if applicable):	CIS-06285-MAJ-06285
Type of Project or Program:	System	Project or program status:	Operational
Date first developed:	July 7, 2007	Pilot launch date:	N/A
Date of last PTA update	February 7, 2023	Pilot end date:	N/A
ATO Status (if applicable):²	Complete	Expected ATO/ATP/OA date (if applicable):	Ongoing Authorization

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	Irina Sidelnikov		
Office:	Office of Information Technology	Title:	OIT Project Manager
Phone:	[REDACTED]	Email:	[REDACTED]

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Minh Vo		
Phone:	N/A	Email:	[REDACTED]

² The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see <https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Documents/DHS%20ATP%20Guide%20v2.0.pdf#search=atp>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 3 of 42

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

The United States Citizenship and Immigration Services submits this updated Privacy Threshold Analysis to document the United States Citizenship and Immigration Services Verification Division and Office of Technology changes to the Systematic Alien Verification for Entitlements Program. The United States Citizenship and Immigration Services administers the Systematic Alien Verification for Entitlements Program, an inter-governmental initiative that provides a web-based service to help federal, state, territorial, tribal and local agencies and other governmental entities verify United States citizenship or immigration status/category information of applicants for benefits, licenses, or other authorized purposes.

This Privacy Threshold Analysis documents that the Systematic Alien Verification for Entitlements Program has

1. Expanded its search capabilities to allow approved Systematic Alien Verification for Entitlements Program user agencies to verify United States citizenship information using Social Security Numbers and other non-Department of Homeland Security enumerators.
2. A new Social Security Administration system connection to support verification of citizenship/immigration status.
3. A new bulk uploader/list processor function that allows user agencies to upload lists of benefit applicants.
4. Use of the Voter Registration and Voter List Maintenance Verification functionality.
5. The collection of information from the Department of State's Consular Consolidated Database/American Citizen Record Query system. Additionally, the Systematic Alien Verification for Entitlements Program will integrate with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data system.

2025 Updates

On April 22, 2025, Homeland Security Secretary Kristi Noem, alongside the United States Citizenship and Immigration Services and the Department of Government Efficiency, announced a comprehensive optimization of the Systematic Alien Verification for Entitlements Program to ensure a single, reliable source for verifying immigration status and United States citizenship nationwide. Congressional, federal, and state stakeholders have periodically expressed interest in using the Systematic Alien Verification for Entitlements to verify naturalized and derived citizenship information during voter registration and/or for voter list maintenance. Verification for voter list maintenance purposes often occurs when a state Department of Motor Vehicles compares its records to state voter agency records to determine if individuals on the voter rolls represented that they were other than U.S. citizens when the Department of Motor Vehicles issued their driver's license. The state voter agency then follows up with those individuals as to their citizenship status through state law voter registration challenge procedures. The United States Citizenship and Immigration Services Verification Division is leading this effort and has identified multiple phases to optimize the program. A high-level summary is provided below, while a more detailed description of each phase follows.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 4 of 42

- Phase 1: Free Service for State, Local, Tribal, Territory agencies and Bulk Uploader. (Estimated completion: Implemented)
- Phase 2: Integration with the Social Security Administration to allow for full Social Security Number to be used as a non-Department of Homeland Security enumerator. (Estimated completion: Implemented)
- Phase 3: Modify the Security Administration integration to allow for truncated Social Security Numbers (last 4-digits) to be used as a non-Department of Homeland Security enumerator. (Estimated completion: July/August 2025)
- Phase 4: Integration with Customs and Border Protection to enable United States passport data, received from the Department of State, to be used within the Systematic Alien Verification for Entitlements Program. (Estimated completion: To be determined)
- Phase 5: Integration with the Department of Justice to enable an incarceration/felony related flag (the flag will be used internally and will not be sent to the agencies or the applicants). (Estimated completion: To be determined)
- Phase 6: Integration with State Driver's Licensing Agencies to enable a Driver License number to be used as a non-Department of Homeland Security enumerator. (Estimated completion: To be determined)

The summary below focuses on phases one (1) through four (4). More detailed information can be found later in this document. Phases five (5) and six (6) are longer term goals of the optimization effort and are still in the exploratory/planning stage. The United States Citizenship and Immigration Services will update this Privacy Threshold Analysis to support the remaining phases during their development.

Phases One (1) through Three (3)

Systematic Alien Verification for Entitlements Program eliminated fees for non-federal users creating Systematic Alien Verification for Entitlements Program cases. User agencies can now create multiple individual cases from a list of data provided by the user. Further, the Systematic Alien Verification for Entitlements Program plans to integrate additional immigration information into search functionality and case results, such as timelines and addresses. Improved automatic status updates and a new user-friendly interface will empower federal, state, local, territorial, and tribal agencies to help prevent individuals who are not qualified for government benefits and licenses from receiving those benefits and licenses. The Department of Homeland Security intends to provide ongoing updates to stakeholders as the Systematic Alien Verification for Entitlements Program Optimization Plan progresses. Systematic Alien Verification for Entitlements Program users must attest to completing the Systematic Alien Verification for Entitlements Program tutorial prior to gaining access to Systematic Alien Verification for Entitlements Program. Users' access is based on their permissions.

The United States Citizenship and Immigration Services has developed and implemented a new bulk uploader/list processor feature to the Systematic Alien Verification for Entitlements Program. This feature will allow program users to upload a list (such as an excel spreadsheet) of benefit applicants to the Systematic Alien Verification for Entitlements Program for processing. Once the list is uploaded, the Systematic Alien Verification for Entitlements Program will accept or not accept the data then, through an automated process, create front-end single-record cases for each entry. Initially the creation of cases using this feature is limited to cases created using an A-number, Citizenship or Naturalization Certificate



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 5 of 42

number, or Social Security number. Agencies will not be prompted to institute additional verification when using this process but are instructed to resubmit additional information when the process is unable to return a response. Expansion of this feature in the future may include the ability to create cases with additional enumerators and the ability to request configured information not automatically selected for the benefit type.

User agencies will be able to access each case created using the list processor feature in the Systematic Alien Verification for Entitlements system as normal, by viewing the individual case status and response. The Systematic Alien Verification for Entitlements Program also has a feature available to all the user agencies to generate a report that will list all the cases created, the status of the case and the Systematic Alien Verification for Entitlements Program response. Access to generate the report, including what cases are included, will vary depending upon the individual user's permission. United States Citizenship and Immigration Services is providing this verification service for all benefit requests. There are approximately 1,200 user agencies with access to the Systematic Alien Verification for Entitlements Program to verify immigration status for benefits or entitlements, and in fiscal year 2024, the Systematic Alien Verification for Entitlements Program completed over 24.5 million first step verifications.

The Systematic Alien Verification for Entitlements Program was originally designed only to use a Department of Homeland Security-issued enumerator (such as an alien number or A-Number) to query immigration records, specifically, to provide immigration status to Systematic Alien Verification for Entitlements Program user agencies. The Systematic Alien Verification for Entitlements Program is now expanding to allow Systematic Alien Verification for Entitlements Program user agencies to provide a Social Security Number or a United States Passport number to query the Systematic Alien Verification for Entitlements Program.

The Systematic Alien Verification for Entitlements Program will also add the ability for user agencies to verify truncated Social Security Numbers (last 4 digits) against Social Security Administration records. This will allow the Systematic Alien Verification for Entitlements Program to verify all United States citizens including those by birth, which was previously not available. A benefit applicant's Social Security number can only be used for automated initial verification and cannot be used for additional verification, which will continue to require a Department of Homeland Security immigration enumerator since the Systematic Alien Verification for Entitlements Program does not normally collect Social Security Numbers or passport numbers. The addition of the Voter Registration and Voter List Maintenance Verification, and the Social Security Administration connection is now live. The Systematic Alien Verification for Entitlements Program can now verify United States-born citizens for voter verification agencies.

The Department of Homeland Security/United States Citizenship and Immigration Services seeks access to Social Security Administration information accessed through the Department of Homeland Security/United States Citizenship and Immigration Services Verification Information System³. The United States Citizenship and Immigration Services and the Social Security Administration agreed to the following limitations on the access to, and disclosure and use of information that identifies a verification request as being generated by United States Citizenship and Immigration Services or associated with a United States Citizenship and Immigration Services program:

³ Verification Information System provides services to customers through Systematic Alien Verification for Entitlements and E-Verify (the latter of which will not be used for this initiative).



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 6 of 42

- Data or information that identifies a verification request as being generated by United States Citizenship and Immigration Services or associated with a United States Citizenship and Immigration Services program will remain information owned by United States Citizenship and Immigration Services.
- The United States Citizenship and Immigration Services will use the verification responses generated by the Social Security Administration only for the purposes described in the Information Sharing Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services and the Social Security Administration.
- Data or information that identifies a verification request as being generated by the United States Citizenship and Immigration Services or associated with a United States Citizenship and Immigration Services program will be used only as provided in the Information Sharing Agreement by the Social Security Administration.
- Data or information that identifies a verification request as being generated by United States Citizenship and Immigration Services or associated with the United States Citizenship and Immigration Services program provided by Social Security Administration will not be duplicated or disseminated outside Social Security Administration without prior written approval from United States Citizenship and Immigration Services. The United States Citizenship and Immigration Services will not give such approval unless the redisclosure is required by law or is essential to the conduct of the exchange. In such cases, the Social Security Administration, the agency redisclosing the records, must specify in writing what records will be redisclosed, to whom they will be redisclosed, and the reasons that justify redisclosure.
- The United States Citizenship and Immigration Services will not duplicate or disseminate the verification responses for a purpose not covered by the Information Sharing Agreement, within or outside of its agency, without the written permission of the Social Security Agreement excepted as required by Federal law. The Social Security Administration will not give such permission, unless Federal law requires disclosure, or disclosure is essential to the purpose of this Agreement. For such permission, The United States Citizenship and Immigration Services must specify in writing what data it is requesting to duplicate or disseminate and to whom, and the reasons that justify such duplication or dissemination.

Administrative Safeguards

The Social Security Administration and the United States Citizenship and Immigration Services will restrict access to the data matched and to any data created by the match to only those users, for example, employees and contractors, who need it to perform their official duties in connection with the uses of the data authorized in the Information Sharing agreement. Further, the Social Security Administration and the United States Citizenship and Immigration Services will advise all personnel with access about the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws.

Parties, including all personnel with access to information, will be appropriately educated and trained regarding the proper handling of personally identifiable information and proper care of the information systems to ensure the overall safeguarding and security of the information. The Social Security Administration and the United States Citizenship and Immigration Services will ensure that its



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 7 of 42

employees, including contractors with the access to any of the information, have completed privacy training on the handling of personally identifiable information.

Phase Four (4)

The United States Citizenship and Immigration Services will need to query other non-United States Citizenship and Immigration Services systems, besides the Social Security Administration's Numident system, with the information provided by the Systematic Alien Verification for Entitlements Program user agency to find the appropriate Department of Homeland Security-issued enumerator to continue with the Systematic Alien Verification for Entitlements Program case processing. For instance, USCIS is researching the possibility of using a United States Passport Number to be able to identify a Department of Homeland Security-issued enumerator. In a case when a User Agency uploads or enters a United States Passport Number instead of a DHS-issued enumerator, the Systematic Alien Verification for Entitlements Program will query another non-United States Citizenship and Immigration Services System using the United States Passport Number along with a unique identifier to find any records and will identify if a Department of Homeland Security-issued enumerator was used by the applicant when applying for a Department of Homeland Security-issued benefit or if a Passport Number was used at a United States Port of Entry and is associated with a Department of Homeland Security-issued enumerator. In this instance, to enable this change, the Systematic Alien Verification for Entitlements Program would integrate with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data to match a Passport Number against Customs and Border Protection and Department of State records to attempt to locate a Department of Homeland Security issued enumerator.

The TECS (not an acronym) - Travel Documents and Encounter Data stores travel document information (scanned images of documents, biographic information, document details, and photographs) from the United States Citizenship and Immigration Services Lawful Permanent Resident Cards along with Department of State-issued United States passports, visas, foreign passports, enhanced driver's licenses, and enhanced tribal cards. The TECS (not an acronym) - Travel Documents and Encounter Data USPassportRESTService allows interconnected systems to query TECS (not an acronym) - Travel Documents and Encounter Data for United States passport information. For this use case, the Systematic Alien Verification for Entitlements Program user agency will input a passport number into the Systematic Alien Verification for Entitlements Program. The query will trigger the USPassportRESTService to locate the matching United States passport number and return the results to the user. This will allow the Systematic Alien Verification for Entitlements Program to verify all types of United States citizens, including those by birth, which was previously not available. Currently, the Systematic Alien Verification for Entitlements Program only collects passport numbers for foreign issued passports if it is provided with an additional Department of Homeland Security enumerator. The United States Citizenship and Immigration Services E-Verify has an existing connection to the USPassportRESTService, which also resides within the Verification Information System, like Systematic Alien Verification for Entitlements Program.

The following are updates that were planned prior to Secretary Noem's vision for optimizing the Systematic Alien Verification for Entitlements Program and are still in progress.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 8 of 42

- Systematic Alien Verification for Entitlements Program will update the responses provided to users as part of the Interface Control Agreement Version 38, which enhances the Systematic Alien Verification for Entitlements Program query logic to provide more accurate information based on the need to know. The Systematic Alien Verification for Entitlements Program will add the collection of an uploaded document such as a Naturalization/Citizenship Certificate Number, when the user submits a second step additional verification, as well as the collection of a reason code, which allows the Systematic Alien Verification for Entitlements Program users to provide additional details regarding the applicant's request, particularly during the additional verification process. The Systematic Alien Verification Entitlements responds to users by providing an immigration status/category or United States citizenship. These additional collections will help Systematic Alien Verification for Entitlements Program identify and remedy data issues, reduce overall manual response times, and allow the Systematic Alien Verification for Entitlements Program to improve the quality of first step automated responses.
- A live site environment will be implemented where Systematic Alien Verification for Entitlements web service users can access new and current interface control agreements. This will streamline the process to update the interface control agreements and ensure that the Systematic Alien Verification for Entitlements Program users have access to the most current information for the Interface Control Agreement Version 38.
- The Systematic Alien Verification for Entitlements Program case response screen will be redesigned so that it is easier to read and allow for the additional information to be submitted. The screen will be packaged in a new way to provide the user clear information during the initial verification.

Additionally, Systematic Alien Verification for Entitlements Program will be collecting information from the Department of State's Consular Consolidated Database / American Citizen Record Query system which is a consular search engine used by the Department of State to manage and access records related to United States citizens, particularly for consular protection and services, including managing passport requests and applications.

2024 Update

As part of the Systematic Alien Verification for Entitlements Program's normal review process, the United States Citizenship and Immigration Services intends to access the Department of State's Consular Consolidated Database / American Citizen Record Query system to verify immigration status of applicants for benefits, licenses, and other authorized purposes. The purpose of collecting this information is to confirm the identity of the applicant to determine their status. This process is part of an ongoing effort that began in 2024.

Background

The Systematic Alien Verification for Entitlements Program is an online service for registered federal, state, territorial, tribal, and local government agencies to verify immigration status and United States citizenship of applicants seeking benefits or licenses. Systematic Alien Verification for Entitlements



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 9 of 42

Program is not a database but queries Department of Homeland Security-accessed federal records to provide registered user agencies with a verification response.

In 1986, Congress mandated that the Immigration and Naturalization Service, now United States Citizenship and Immigration Services, establish a system to verify the citizenship and immigration status of individuals seeking government benefits and licenses.

The United States Citizenship and Immigration Services Verification Division administers the Systematic Alien Verification for Entitlements Program, which is an intergovernmental initiative using a web-based service to help federal, state, territorial, tribal and local benefit-issuing and licensing agencies and other governmental entities determine the immigration status or United States citizenship of applicants for public benefits, licenses, grants, credentials, background investigations, and other lawful purposes, so only entitled applicants receive them. Systematic Alien Verification for Entitlements Program verifies immigration status/category and United States citizenship against Department of Homeland Security-accessed records. Historically, the Systematic Alien Verification for Entitlements Program has not verified information for United States born citizens as a Department of Homeland Security immigration enumerator was previously required, but now the Systematic Alien Verification for Entitlements Program can verify United States-born United States citizens against Social Security Administration data. The Systematic Alien Verification for Entitlements Program does not determine an applicant's eligibility for a specific benefit or license, as this is the responsibility of the benefit/license granting agency.

As of April 1, 2025, the Systematic Alien Verification for Entitlements Program has revised its transaction charges for all state, local, tribal, and territorial government agencies using the Systematic Alien Verification for Entitlements Program to eliminate those charges. Federal agencies are still charged a fee to use the Systematic Alien Verification for Entitlements Program. The authority for the Systematic Alien Verification for Entitlements Program, and for particular Systematic Alien Verification for Entitlements Program authorized uses can be found in the Immigration Reform and Control Act⁴; the Personal Responsibility and Work Opportunity Reconciliation Act⁵ Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996⁶, and the REAL ID Act of 2005⁷, the Patient Protection and Affordable Care Act of 2010,⁸ and the Federal Aviation Administration Extension, Safety and Security Act of 2016.⁹ In addition, the Systematic Alien Verification for Entitlements Program has an obligation under 8 U.S.C. 1373(c) to "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."

⁴ Immigration Reform and Control Act of 1986, Public Law No. 99-603

⁵ Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Public Law No. 104-193, 110 Statute 2168

⁶ Title IV, Subtitle A, of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 Public Law 104-208, 110 Statute 3009

⁷ REAL ID Act of 2005, Public Law No. 109-13, 119 Statute 231

⁸ Patient Protection and Affordable Care Act of 2010, Public Law No. 111-148

⁹ Federal Aviation Administration Extension, Safety and Security Act of 2016 (Federal Aviation Administration Act), Public Law No. 114-190 § 3405(d) (July 15, 2016).



The United States Citizenship and Immigration Services Verification Division operates the Verification Data Information System as the search engine for Systematic Alien Verification for Entitlements Program and the E-Verify Program. The Verification Data Information System accesses nationally accessible databases of selected immigration records to support both the Systematic Alien Verification for Entitlements Program and the E-Verify Program. The Systematic Alien Verification for Entitlements Program queries an individual's immigration status to help the administering agency determine eligibility for any public benefit, license, or credential based on their United States citizenship or immigration status. The United States Citizenship and Immigration Services is obligated by law to 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.

Systematic Alien Verification for Entitlements Program

The United States Citizenship and Immigration Services administers the Systematic Alien Verification for Entitlements Program, an inter-governmental initiative that provides a web-based service to help federal, state, territorial, tribal, and local benefits-issuing and licensing agencies and other governmental entities along with Airport Operators verify the United States citizenship and immigration status/category information of applicants for public benefits or licenses (hereinafter "benefits"). Examples of these benefits include Supplemental Security Income Supplemental Nutrition Assistance Program (formerly food stamps), Temporary Assistance for Needy Families cash assistance, Medicaid, Children's Health Insurance Program, REAL ID compliance, and other statutorily authorized purposes, including voter verification.

The Systematic Alien Verification for Entitlements Program also eliminates fees for database searches, breaks down silos for more accurate results, streamlines List Processor submission, and integrates additional immigration information, such as timelines and addresses. Automatic status updates and a new user-friendly interface will empower Federal, state, local, territorial, and tribal agencies to help prevent individuals who are not qualified for government benefits from receiving those benefits. The Department of Homeland Security intends to provide ongoing updates to stakeholders as the Systematic Alien Verification for Entitlements Program Optimization Plan progresses.

Agency use of the Systematic Alien Verification for Entitlements Program is administered by the Verification Division. All user agencies are required to register with the Systematic Alien Verification for Entitlements Program to access the system prior to using the Systematic Alien Verification for Entitlements Program. The Systematic Alien Verification for Entitlements Program is not a source system and connects with federal immigration systems, and now the Social Security Administration's Numident¹⁰ system, to access applicable information. The Systematic Alien Verification for Entitlements Program also has a Case Status Check capability that allows benefit applicants to view the status of their Systematic Alien Verification for Entitlements Program case. The system provides benefit eligibility checks based on the grant dates. The Verification Division has a three (3) tier process when verifying an individual's immigration status or United States citizenship.

¹⁰ NUMIDENT or "Numerical Identification" refers to the master file of Social Security Administration records containing information about individuals who have applied for or been assigned a Social Security Number. This file includes records for applications, claims, and death records related to individuals with a Social Security Number.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 11 of 42

Users must perform all additional verification procedures the Systematic Alien Verification for Entitlements Program requires and/or the applicant requests prior to denying a benefit based upon a Systematic Alien Verification for Entitlements Program response. Users must provide all applicants who are denied benefits based solely or in part upon the Systematic Alien Verification for Entitlements Program response adequate written notice and the information necessary to contact the Department of Homeland Security so that applicants may correct their immigration records in a timely manner, if necessary.

Initial verification

A Systematic Alien Verification for Entitlements Program user agency accesses their account in the system and either submits requests individually or via a bulk request using the system's new bulk uploader feature. When a Systematic Alien Verification for Entitlements Program user agency submits an online verification request for a benefit applicant, it provides several required identifiers for the benefit applicant from documents presented by the benefit applicant, including first and last name, date of birth, and at least one of the following: an enumerator from the Department of Homeland Security (e.g. Alien number/United States Citizenship and Immigration Services number, Form I-94 Number, Card Number/I-797 Receipt number, Citizenship/Naturalization Certificate Numbers), a Social Security number from Social Security Administration, or a United States passport number from the Department of State. Social Security Numbers and United States passport numbers are new enumerators. Previously, enumerators were solely limited to Department of Homeland Security-issued immigration enumerators.

In the case of a bulk upload the Systematic Alien Verification for Entitlements Program will use an automated process to create individual cases for each benefit applicant on the list.

Using these data fields, the Systematic Alien Verification for Entitlements Program performs an automated query of various Systematic Alien Verification for Entitlements Program-accessed federal databases for relevant records. If a Social Security Number is submitted under this new collection, the Systematic Alien Verification for Entitlements Program will verify this enumerator against the Social Security Administration records, including the Social Security Administration death records and citizenship records. If the individual's Social Security account has a record of an A-number or certificate number, the Social Security Administration will provide that information to the Systematic Alien Verification for Entitlements Program, which will be used to validate that information against the Department of Homeland Security records. If a United States passport number is submitted, the Systematic Alien Verification for Entitlements Program will verify it against the Department of State related records available in the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data system. When the Systematic Alien Verification for Entitlements Program locates a record pertaining to the benefit applicant in any of these federal databases, the Systematic Alien Verification for Entitlements Program displays a verification response to the user agency within seconds.

Second step, additional verification (Tier 2)



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 12 of 42

If the Systematic Alien Verification for Entitlements Program is unable to find a record pertaining to the benefit applicant through the automated first level search of the Department of Homeland Security records, including United States passport records and the Social Security Administration records, it displays a response to the user indicating additional action is required from the user agency, including requesting additional verification when an immigration enumerator is available. If only a Social Security Number is submitted for verification, the user agency will be informed to close the case and submit a new request using either corrected data or an immigration enumerator, since additional verification cannot be conducted with only a Social Security Number.

The Systematic Alien Verification for Entitlements Program user agency may start the additional verification procedure, which may include is an in-depth manual review by Systematic Alien Verification for Entitlements Program staff (Status Verification Analyst) to determine the applicant's immigration status or United States citizenship. At the point at which the "Institute Additional Verification" message is displayed, user agencies must submit the case for additional verification if they are relying on a Systematic Alien Verification for Entitlements Program response to deny a benefit. Additionally, if the user agency receives a response and they have questions about the validity of the response, the user agency may submit a case that already received a Systematic Alien Verification for Entitlements Program response for additional verification. Users must also submit a case for additional verification when requested by the applicant.

User agencies may not rely on a Systematic Alien Verification for Entitlements Program response to approve or deny an application for benefits unless they have followed all required Systematic Alien Verification for Entitlements Program verification procedures. The Systematic Alien Verification for Entitlements Program users are not required to institute additional verification if a user agency has alternate grounds upon which to base its decision to decide a benefit that do not require verification of the applicant's immigration status/category, even where the agency is prompted to do so. Examples of when a user agency has alternate grounds to base a decision that does not require the completion of additional verification include:

- The applicant does not meet eligibility requirements for the benefit unrelated to immigration status/United States citizenship.
- The applicant withdraws their application.
- The applicant cannot be contacted/fails to respond to an agency's request for follow-up.
- The applicant presents documentation the Systematic Alien Verification for Entitlements Program cannot verify (such as a military identification).

This revision adds the collection of an uploaded document which includes immigration enumerators (such as a Form I-94, Arrival/Departure Records, Naturalization/Citizenship Certificate, or passport records) when a case is submitted for second step additional verification as well as a reason code. Reason codes can provide information on why the initial verification was not successful, if the case has been escalated for additional verification, or suggest that additional verification steps may be needed to determine the applicant's status or eligibility for a benefit. Reason codes can also identify if it was a user-initiated additional verification request when the user received an initial Systematic Alien Verification for Entitlements Program response providing an immigration status/category or United States citizenship. These additional collections will help the Systematic Alien Verification for Entitlements Program identify



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 13 of 42

and remedy data issues, reduce overall manual response times, and allow the Systematic Alien Verification for Entitlements Program to improve the quality of first step automated responses.

If the second step manual search produces relevant information enabling the verification of immigration status, the Systematic Alien Verification for Entitlements Program provides an electronic response to the inquiring user agency.

If the user agency declines second step additional verification, the verification process ceases. Additional screens notify the user agency that closing the case without performing additional verification means the agency does not have a complete Systematic Alien Verification for Entitlements Program response. The Systematic Alien Verification for Entitlements Program user agencies cannot rely upon an incomplete Systematic Alien Verification for Entitlements Program response to deny a benefit.

Third step Additional Verification with Documents (Tier 3)

If a benefit applicant's immigration status/category cannot be verified on initial or additional verification step when submitting a Department of Homeland Security enumerator, the system will prompt the user agency to resubmit the case with documents. When the prompt is received, the agency must upload a copy of the front and back of the immigration document the applicant presented to the user agency for the Systematic Alien Verification for Entitlements Program to perform detailed manual research at third step. A Department of Homeland Security immigration enumerator is required for the third step additional verification. The Systematic Alien Verification for Entitlements Program cannot complete third step additional verification using non-immigration documentation. The Systematic Alien Verification for Entitlements Program user agencies are legally authorized to make electronic copies of immigration documents for purposes of verifying immigration status. Cases created with just the Social Security Number or a Passport Number as the enumerator are not subject to this step.

If the third step manual review produces relevant information enabling the verification of immigration status/category or United States citizenship, the Systematic Alien Verification for Entitlements Program provides an electronic response to the user agency.

If a benefit applicant's immigration status/category is not verified after completing third step verification, the Systematic Alien Verification for Entitlements Program will provide additional information or guidance on how to proceed.

If the applicant believes their information in the Department of Homeland Security records is incorrect, the applicant can seek a records correction. User agencies should provide the Systematic Alien Verification for Entitlements Program Fact Sheet and Systematic Alien Verification for Entitlements Program Records: Fast Facts for Benefit Applicants¹¹ to benefit applicants that may require records correction.

¹¹ The Systematic Alien Verification for Entitlements Fact Sheet and Systematic Alien Verification for Entitlements Records: Fast Fact for Benefits Applicants is accessible at <https://www.uscis.gov/save/benefit-and-license-applicants/resources-for-benefit-and-license-applicants>



The Systematic Alien Verification for Entitlements Program user agency continues to have the option of running a web report within the system that will create a file in Adobe format of all cases processed for their organization. The United States Citizenship and Immigration Services provides access to relevant reports of approved or pending cases for Systematic Alien Verification for Entitlements Program user agencies to assist them in managing their Systematic Alien Verification for Entitlements Program cases and monitoring their own compliance with the Systematic Alien Verification for Entitlements Program rules and the federal deeming and reimbursement rules. User agencies can run case-specific reports for quality assurance that will include information, such as name, date of birth, type of benefit, immigration identifier (e.g., A-Number, unexpired foreign passport number, I-94 Arrival/Departure Record), and immigration status, only if the benefit was administered.

Voter Registration and Voter List Maintenance Verification

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 expanded the Systematic Alien Verification for Entitlements Program by requiring the program to respond to inquiries by federal, state and local government agencies seeking to verify or determine the citizenship or immigration status of any individual within the jurisdiction of the agency for any lawful purpose. See 8 U.S.C. § 1373(c). This authority allows agencies to use the Systematic Alien Verification for Entitlements Program for verification of citizenship and immigration status outside of the traditional benefit-granting programs covered by the Immigration Reform and Control Act of 1986. This includes voter registration and voter list maintenance purposes, so long as the agency meets the legal requirements for using the Systematic Alien Verification for Entitlements Program and provides the required applicant information, when submitting verification requests.

On January 20, 2025, and March 25, 2025, the President issued Executive Orders 14159, *Protecting the American People Against Invasion*¹² and 14248, *Preserving and Protecting the Integrity of American Elections*¹³ respectively. Executive Order 14159 requires the Secretary to “promptly issue guidance to ensure maximum compliance by [Department of Homeland Security] personnel with the provisions of 8 U.S.C. 1373¹⁴ and 8 U.S.C. 1644¹⁵ and ensure that State and local governments are provided with the information necessary to fulfill law enforcement, citizenship, or immigration status verification requirements authorized by law.” Executive Order 14248¹⁶ provides, “Federal laws, such as the National Voter Registration Act (Pub. L. 103-31) and the Help America Vote Act (Pub. L. 107-252), require States to maintain an accurate and current Statewide list of every legally registered voter in the State. Pursuant to the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Department of Homeland Security/United States Citizenship and Immigration Services is required to share database information with States upon request so they can fulfill this duty. 8 U.S.C. 1373(c)¹⁷.” Executive Order 14159¹⁸ directs the Secretary to “ensure that State and local officials have, without the requirement of the payment

¹² <https://www.federalregister.gov/documents/2025/01/29/2025-02006/protecting-the-american-people-against-invasion>

¹³ <https://www.federalregister.gov/documents/2025/03/28/2025-05523/preserving-and-protecting-the-integrity-of-american-elections>

¹⁴ 8 USC 1373 Communication between government agencies and the Immigration and Naturalization Service

¹⁵ 8 USC 1644 Communication between State and local government agencies and Immigration and Naturalization Service

¹⁶ Executive Order 14248 Preserving and Protecting the Integrity of American Elections

¹⁷ 8 USC. 1373(c) Obligation to respond to inquiries

¹⁸ Executive Order 14159 Protecting the American People Against Invasion



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 15 of 42

of a fee, access to appropriate systems for verifying the citizenship or immigration status of individuals registering to vote or who are already registered.” The Secretary is also required under Executive Order 14159, in coordination with the Department of Government Efficiency Administrator, to review each State’s publicly available voter registration list and available records concerning voter list maintenance activities as required by 52 U.S.C. 20507¹⁹, alongside Federal immigration databases and State records requested, including through subpoena where necessary and authorized by law, for consistency with Federal requirements. To support this activity the Attorney General is required to prioritize enforcement of 18 U.S.C. 611²⁰ and 1015(f)²¹ and similar laws that restrict aliens from registering to vote or voting, including through use of: (i) databases or information maintained by the Department of Homeland Security; (ii) State-issued identification records and driver license databases; and (iii) similar records relating to citizenship.

In accordance with federal statutes and policies, the Department of Homeland Security personnel must, in a timely manner, provide verification or immigration status information in response to inquiries from State and local government agencies to verify or ascertain the citizenship or immigration status of individuals. As required by 8 U.S.C. 1373(c), such inquiries must relate to individuals within the jurisdiction of the State or local government agency and must be for a purpose authorized by law. Department of Homeland Security personnel have been directed to comply, to the maximum extent possible and permissible under law, with Section 1373, considering federal statutory requirements, including the Privacy Act of 1974, 5 U.S.C. 552a²², and 8 U.S.C. 1367²³ (special protected class information); as well as other laws, rules, regulations, policies, and requirements regarding verification, information sharing, and confidentiality.

The Systematic Alien Verification for Entitlements Program user agency registration process determines whether a state voter registration agency meets the legal requirements for using the Systematic Alien Verification for Entitlements Program. As part of registering to use Systematic Alien Verification for Entitlements Program, the agency must provide the Systematic Alien Verification for Entitlements Program all applicable legal authorities and voter registration procedures that authorize the agency to engage in voter registration and/or voter list maintenance activities and verify citizenship status before making individual determinations regarding eligibility for voter registration. The United States Citizenship and Immigration Services provides information on its public facing website to assist user agencies understand the above referenced requirements.²⁴

Current Process - Voter Registration and Voter List Maintenance Verification

¹⁹ 52 USC 20507 Requirements with respect to administration of voter registration

²⁰ 18 USC 611 Voting by aliens

²¹ 18 USC 1015 (f) Naturalization, citizenship or alien registry, whoever knowingly makes any false statement or claims that he is a citizen of the United States in order to register to vote or to vote in any Federal, State, or local election (including an initiative, recall, or referendum)-Shall be fined under this title or imprisoned not more than five years, or both

²² 5 USC 552a Records maintained on individuals

²³ 8 USC 1367 Penalties for disclosure of information

²⁴ The Systematic Alien Verification for Entitlements Voter Registration and Voter List Maintenance Fact Sheet is accessible at <https://www.uscis.gov/save/resources/voter-registration-and-voter-list-maintenance-fact-sheet>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 16 of 42

In understanding the use of the Systematic Alien Verification for Entitlements Program for voter verification-related purposes (voter registration and voter list maintenance), one should also bear in mind the following limitations and considerations:

- The information needed to verify an individual through the Systematic Alien Verification for Entitlements Program is typically not collected on a voter registration application, although it may be available from other sources, especially driver's license applications.
- The Systematic Alien Verification for Entitlements Program previously was only able to verify United States citizenship for naturalized and certain acquired citizens²⁵ for whom the United States Citizenship and Immigration Services has a record of their citizenship.
- The Systematic Alien Verification for Entitlements Program previously was often unable to verify acquired United States citizens because eligible individuals frequently do not apply for and thus do not receive a determination and certificate of United States citizenship from the United States Citizenship and Immigration Services.
- Department of State adjudicates acquired citizens that may not have a record with the United States Citizenship and Immigration Services via the issuance of U.S. passports. Therefore, obtaining passport information from the Department of State is in progress.
- The Department of State maintains records for individuals who have renounced their citizenship. Once a Certificate of Loss of Nationality is approved by the Department of State indicating the official determination of loss of United States nationality, this information is shared with the United States Citizenship and Immigration Services per 8 USC 1373.²⁶
- With the newly established connection to the Social Security Administration's Numident system, the Systematic Alien Verification for Entitlements Program is now able to verify more United States citizens, including United States citizens by birth, when a Social Security Number is provided.

Verification for voter list maintenance purposes often occurs when a state Department of Motor Vehicles compares its records to the state voter agency records to determine if any individuals on the voter rolls identified that they were non-United States citizens when the Department of Motor Vehicles issued their driver's license. The state voter agency would then follow up with those individuals their citizenship status through established state law voter registration challenge procedures. As part of the established voter registration challenge procedures, the State Voter Agency will seek to establish the immigration/citizenship status of the individuals and use Systematic Alien Verification for Entitlements Program as one method to verify the information.

There are likely some situations in which the Systematic Alien Verification for Entitlements Program provides an initial response indicating a non-United States citizen immigration status (e.g., Lawful Permanent Resident) when the registrant is in fact a United States citizen. However, as also noted above, rules for using the Systematic Alien Verification for Entitlements Program prohibit voter registration agencies from relying upon this initial verification response to deny or revoke registration since as by

²⁵ "Acquired citizenship" refers to U.S. citizenship conveyed to children through the naturalization of parents or, under certain circumstances, at birth to foreign-born children of U.S. citizens, provided certain conditions are met.

²⁶ 8 USC 1873 outlines the communication between government agencies and the Immigration and Naturalization Service.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 17 of 42

asserting United States citizenship as part of registering to vote, registrants inherently disagree with any initial response indicating they are not a United States citizen.

Shortfalls in data accuracy in the system could cause incomplete or false results.

According to Systematic Alien Verification for Entitlements Program subject matter experts, the situations in which the Systematic Alien Verification for Entitlements Program provides an initial non-United States citizen immigration status for a United States citizen who has a certificate of naturalization or citizenship from the United States Citizenship and Immigration Services, or legacy Immigration and Naturalization Service can happen for a variety of reasons. In some instances, the initial non-United States citizen response is due to the lack of an electronic record with the Social Security Administration showing United States citizenship (which was not reliably recorded pre-1981), or the lack of an electronic record of a United States Citizenship and Immigration Services naturalization or acquired citizenship certificate, which is more likely for older certificates issued before recording them in electronic systems became a consistent practice. In addition, although the electronic record-matching algorithms in the United States Citizenship and Immigration Services Person Centric Service that the Systematic Alien Verification for Entitlements Program uses are very good, the United States Citizenship and Immigration Services previously identified and subsequently fixed two algorithm issues that caused Systematic Alien Verification for Entitlements Program to provide an initial verification response of Lawful Permanent Resident for some naturalized citizens and a small number of acquired United States citizens. But again, many of the safeguards noted above are designed to address any imperfections in records and algorithms used to match them.

The delay between the issuance a Certificate of Naturalization during a naturalization ceremony and when the certificate is reflected in source systems and made available to the Systematic Alien Verification for Entitlements Program rarely, if ever, causes the Systematic Alien Verification for Entitlements Program to provide an initial response of non-United States citizen immigration status. It typically takes about one business day plus a few hours for an electronic record of the certificate to be available to the Systematic Alien Verification for Entitlements Program once it is input by the responsible United States Citizenship and Immigration Services office. The Systematic Alien Verification for Entitlements Program rarely, if ever, receives requests to verify United States citizenship during this time.

Additionally, the United States Citizenship and Immigration Services is not the source agency for Social Security Administration related information. While the United States Citizenship and Immigration Services assumes the accuracy of the Social Security Administration data, it cannot verify accuracy of the information and relies on the Social Security Administration to ensure the data accuracy, timeliness, and integrity of their own data.

Customs and Border Protection Integration

The Systematic Alien Verification for Entitlements Program will integrate with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data. Customs and Border Protection is now permitting the Systematic Alien Verification for Entitlements Program to query TECS (not an acronym) Travel Documents and Encounter Data system to find a match to US passport information in Customs and Border Protection holdings. The TECS (not an acronym) - Travel Documents and Encounter Data system stores travel document information (i.e. scanned images of documents, biographic information, document details, and photographs) from the United States Citizenship and Immigration Services Lawful Permanent Resident Cards, Department of State-issued United States



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 18 of 42

passports and visas, foreign passports, enhanced driver's licenses, and enhanced tribal cards. The TECS (not an acronym) - Travel Documents and Encounter Data USPassportRESTService allows interconnected systems to query TECS (not an acronym) - Travel Documents and Encounter Data for United States passport information. For this use case, the Systematic Alien Verification for Entitlements Program user agencies will input a United States passport number into the Systematic Alien Verification for Entitlements Program system.

The query will trigger the USPassportRESTService to locate the matching United States passport number and return the results to the user. This will allow the Systematic Alien Verification for Entitlements Program to verify all types of United States citizens, including those by birth, which was previously not available. Currently, the United States Citizenship and Immigration Services E-Verify Program has an existing connection to the USPassportRESTService, which also resides within the Verification Information System, like the Systematic Alien Verification for Entitlements Program.

Customs and Border Protection has the authority to collect passport photos pursuant to 5 USC 552a (4).²⁷ Customs and Border Protection receives a routine feed from the Department of State with US passports as they are issued and/or updated. Customs and Border Protection also collects passport information primarily on all travelers seeking to enter the United States at ports of entry. Customs and Border Protection uses this information as part of Agency operations.

Social Security Administration Data Sharing

The Information Sharing Agreement between the Department of Homeland Security-United States Citizenship and Immigration Services and the Social Security Administration documents the Social Security Administration's support by matching data submitted through the Systematic Alien Verification for Entitlements Program to Social Security Administration records in the Social Security Administration's master files of Social Security Number holders and Social Security Number Applications. The United States Citizenship and Immigration Services will only submit verification requests to the Social Security Administration for authorized purposes.

The United States Citizenship and Immigration Services Verification Division and Social Security Administration connection is now live and now connects the Systematic Alien Verification for Entitlements Program with the Social Security Administration's Numident system. Prior to the connection, the United States Citizenship and Immigration Services and Social Security Administration executed a Letter of Agreement that identifies the authorities for both organizations as well as purposes and the data exchange. The United States Citizenship and Immigration Services will document this sharing in a separate Privacy Threshold Analysis.

The Systematic Alien Verification for Entitlements Program performs an automated query of various Systematic Alien Verification for Entitlements Program-accessed federal databases for relevant records. Now, if a Social Security Number is submitted by a user agency, the Systematic Alien Verification for Entitlements Program will verify this enumerator against the Social Security Administration Numident system including the death and citizenship records. If the individual's Social Security account has a record of an A-number or certificate number, the Social Security Administration will provide that information to the Systematic Alien Verification for Entitlements Program, which will in turn be used to

²⁷ 5 USC 552a (4) Records maintained on individuals - collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 19 of 42

<p>validate the information against the Department of Homeland Security records. Verifying citizenship status using Social Security Administration data will be made available to all Systematic Alien Verification for Entitlements Program user agencies.</p> <p><u>Department of State Data Sharing</u></p> <p>If a United States passport number is submitted, the Systematic Alien Verification for Entitlements Program will verify it against information from Department of State-issued passports maintained by the Custom Boarder Protection. Additionally, Systematic Alien Verification for Entitlements Program will collect information from the Department of State’s Consular Consolidated Database / American Citizen Record Query system, which is a consular search engine used by the Department of State to manage and access records related to United States citizens, particularly for consular protection and services, including managing passport requests and applications.</p> <p>Department of Homeland Security-Department of State Memorandum of Agreement Appendix A allows this query of passport information to be used in Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data to support its missions, including but not limited to verification of United States passports, whenever the document is presented as proof of identity to obtain a benefit, privilege, status, or credential from the Department of Homeland Security, for vetting and screening purposes, and/or for transportation security, national security, law enforcement, border security (including biometric entry and exit initiatives), immigration (including verification purposes such as E-Verify) and counterterrorism purposes.</p> <p><u>User Agencies Memoranda of Agreement</u></p> <p>All user agency memorandums of agreements contain similar provisions to protect the due process and other rights of individuals for whom states or other user agencies submit verification requests to the Systematic Alien Verification for Entitlements Program²⁸. The United States Citizenship and Immigration Services has an online tool that allows the public to search if a federal, state, local, tribal, or territorial agency is registered with the Systematic Alien Verification for Entitlement Program.²⁹</p>	
<p>2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? <i>Please check all that apply.</i></p>	<p><input type="checkbox"/> This project does not collect, collect, maintain, use, or disseminate any personally identifiable information³⁰</p> <p><input checked="" type="checkbox"/> Members of the public</p>

²⁸ The Systematic Alien Verification for Entitlements Program memorandum of agreement is assessable at <https://www.uscis.gov/save/prospective-user-agencies/register-an-agency-for-save> and under the “How to Register for SAVE” section.

²⁹ The Systematic Alien Verification for Entitlement Program search tool is accessible at <https://www.uscis.gov/save/save-agency-search-tool>.

³⁰ DHS defines personal information as “Personally Identifiable Information” or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. “Sensitive PII” is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 20 of 42

	<input checked="" type="checkbox"/> U.S. Persons (U.S citizens or lawful permanent residents) <input checked="" type="checkbox"/> non-U.S. Persons <input checked="" type="checkbox"/> DHS Employees/Contractors (list Components): United States Citizenship and Immigration Services <input type="checkbox"/> Other federal employees or contractors (list agencies): <i>Click here to enter text.</i>
<p>2(a) Is information meant to be collected from or about sensitive/protected populations?</p>	<input type="checkbox"/> No <input checked="" type="checkbox"/> 8 USC § 1367 protected individuals (e.g., T, U, VAWA) ³¹ <input checked="" type="checkbox"/> Refugees/Asylees <input type="checkbox"/> Other. Please list:
<p>3. What specific information about individuals is collected, maintained, used, or disseminated?</p>	
<p><u>Information Collected from Requesting Agencies about applicants for benefits, licenses, or other authorized purposes:</u></p> <ul style="list-style-type: none"> • Full Name • Date of birth • Benefit sought • Driver license • State Identification • Citizenship or nationality • Country of birth • A-Number • Social Security Number • Alias • Customer Agency-issued Case Number <p><u>Unique Immigration Identifiers Used:</u></p>	

³¹ This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, available at <http://dhsconnect.dhs.gov/org/comp/mgmt/policies/Directives/002-02.pdf>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 21 of 42

- Alien number
- United States Citizenship and Immigration Services Number
- I-94 Admission Record Number (a 11-digit admission record assigned to foreign visitors entering the United States by the United States Customs and Border Protection)
- Student and Exchange Visitor Information System Identification Number
- Naturalization or Citizenship Certificate Number
- Card Number / I-797 Receipt Number (unique identifier assigned by the United States Citizenship and Immigration Services to track an immigration application or petition).
- Visa Number
- Foreign passport number (if submitted with another immigration enumerator and issuing country)

Other Identifiers:

- Social Security Number including a truncated version of the Social Security Number where only the last four digits are displayed, with the initial five digits are masked using asterisks (*) or XXXXX
- United States Passport Number
- Agency Data Universal Numbering System

Other Information:

Additional information requested by the agency:

- Employment Authorization Document History
- Grant Date
- Affidavit of Support Sponsor Data³²
 - Full name
 - Current mailing address - In care of name (if any)
 - Current physical address
 - Country of domicile
 - Date of birth
 - Country of birth
 - Social Security Number
 - Immigration Status
 - Sponsors A-number (if any)
 - United States Citizenship and Immigration Services Online Account Number (if any)
 - Military service
 - Employment and income
 - Federal tax return information

³² A United States Citizenship and Immigration Services Affidavit of Support sponsor is an individual who signs a legal contract, Form I-864, agreeing to financially support an intending immigrant, ensuring they won't become a public charge. This sponsor is typically the U.S. citizen, lawful permanent resident, or U.S. national who filed the immigrant petition.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 22 of 42

- Sponsor Deeming and Agency Reimbursement Information Collection
 - Whether the benefit-granting agency approved or denied the application for the means-tested public benefit.
 - If the benefit-granting agency denied the application, if the denial was based upon the information that the Systematic Alien Verification for Entitlements Program provided in its response to the citizenship and immigration status verification request from the benefit-granting agency.
 - Whether the benefit-granting agency deemed sponsor/household member income and, if not, the exception or reason for not doing so.
 - Whether the benefit-granting agency sent the sponsor a reimbursement request letter (yes/no).
 - Whether the sponsor complied with his or her reimbursement obligation.
 - Whether the benefit-granting agency conducted a collection action or other proceedings if the sponsor did not comply with his or her reimbursement obligation (yes/no and if yes, the status, court or forum, and docket or matter number).
- Data collected on Form I-864, Affidavit of Support Under Section 213A of the Immigration and Nationality Act
 - Principal Immigrant:
 - Full name
 - Current mailing address - In care of name (if any)
 - Current physical address
 - Country of Citizenship or Nationality
 - Date of birth
 - Alien Registration number
 - United States Citizenship and Immigration Services Online Account Number (if any)
 - Daytime telephone number
 - Principal Immigrant Family Members:
 - Full name
 - Relationship to Principal Immigrant
 - Alien Registration number
 - United States Citizenship and Immigration Services Online Account Number (if any)
 - Daytime telephone number
 - Interpreter's Contact Information, Certification and Signature:
 - Full name
 - Telephone number
 - Email address (if any)
 - Interpreter's certification and signature
 - Preparer's Contact Information:
 - Daytime number
 - Mobile number (if any)
 - Email address (if any)
 - Signature
- Cuban/Haitian, Immigration Status



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 23 of 42

- Violence Against Women's Act
- Request Document Review
- Citizenship Status
- Immigration Documentation (uploaded by the user agency to perform additional verification)

Agency User Information

- Agency point of contact name
- Agency point of contact phone number
- Initiated on
- Initiated by

Information Shared with Social Security Administration:

- Full Name
- Date of Birth
- Social Security Number

DATA Received and Maintained from Social Security Administration:

- Social Security Number Match: True/False
- Name Match: True/False
- Date of Birth Match: True/False
- Citizenship Indicator:
 - "A" - United States citizen
 - "B" - Legal alien, eligible to work
 - "C" - Legal alien, not eligible to work
 - "D" - Other
 - "E" - Alien Student - restricted work authorized
 - "F" - Conditionally legalized alien
- Foreign Born Indicator: Citizenship code is not present, but individual was foreign born
- Alien Registration Number: Where applicable
- Certificate Number: Where applicable
- Death Indicator: Yes Deceased / Not Deceased
- Error Code Descriptions: Transaction and record levels

Information Shared with TECS (not an acronym) – TECS (not an acronym)-Travel Documents and Encounter Data for Passport query:

- Full Name
- Date of Birth
- United States passport number



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 24 of 42

Information Provided to Requesting User Agencies:

- Case Verification Number: a Systematic Alien Verification for Entitlements Program generated number
- Initial Request Date
- Identification Type
- Identification Number
- Last Name
- Benefit Code
- Benefit Description
- Initial Request Response: Lawful Status, No Lawful Status, Deceased
- Additional Request Date
- Additional Request Response: Lawful Status, No Lawful Status, Deceased
- Third Step Request Date
- Third Step Resolution: Lawful Status, No Lawful Status, Deceased

Additional information for immigrants requested from agencies for which they established the authority/need to receive

- Employment authorization document history
- Grant date
- Affidavit of Support Sponsor Data
- Cuban/Haitian Entrant Information
- Violence Against Women’s Act information
- Immigration Status
- Request document review
- Citizenship status
- Photo
- Closed Date
- Receipt number

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?³³ If applicable, check all that apply.

³³ Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, available at <https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information>.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 25 of 42

<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Social Security number <input checked="" type="checkbox"/> Alien Number (A-Number) <input type="checkbox"/> Tax Identification Number <input checked="" type="checkbox"/> Visa Number <input checked="" type="checkbox"/> Passport Number <input type="checkbox"/> Bank Account, Credit Card, or other financial account numbers 	<ul style="list-style-type: none"> <input type="checkbox"/> Social Media Handle/ID <input checked="" type="checkbox"/> Driver's License/State ID Number <input type="checkbox"/> Biometric identifiers (e.g., <i>FIN, EID</i>) <input checked="" type="checkbox"/> Biometrics.³⁴ <i>Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.</i> <input checked="" type="checkbox"/> Other. <i>Please list:</i> Form I-94 number, Student and Exchange Visitor Information System Identification number, Naturalization / Citizenship Certificate number, Permanent Resident Card number / Receipt number, and Visa number.
<p>3(b) Please provide the specific legal basis for the collection of SSN:</p>	<p>The Social Security Number is collected from applicants and is used to verify their immigration status/United States citizenship. div. C, title VI, Section 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-707, codified at 8 U.S.C. 1373 (a) and (c). Authority for having a system for verification of citizenship and immigration status of individuals seeking government benefits is governed by the Immigration Reform and Control Act of 1986 Pub. L. No. 99-603, 100 Stat. 3359.</p> <p>Sections 415 and 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, authorizes the collection and use of Social Security Numbers to verify entitlement to public benefits, licenses, and credentials.</p>
<p>3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.</p>	
<p>The Social Security Number is used to assist in identity verification for user agencies and in determining benefits eligibility. If possible, the United States Citizenship and Immigration Services will use a truncated Social Security Number if provided by the user agency.</p>	

³⁴ If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 26 of 42

<p>3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, <i>SSN Collection and Use Reduction</i>,³⁵ which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: <i>even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.</i></p>
<p>The United States Citizenship and Immigration Services has traditionally used an alternative number to the Social Security Number to access records to determine the citizenship/immigration status of user agencies benefit applicants in compliance with the Department of Homeland Security privacy-related policies. However, United States Citizenship and Immigration Services now needs to collect Social Security numbers to facilitate user agencies' ability to submit a request for citizenship/immigrations status of benefit applicants. The United States Citizenship and Immigration Services is working to implement use of the truncated form of a Social Security number (i.e. the last four numbers of a Social Security number rather than the full identifier) to retrieve information from the Social Security Administration. The Systematic Alien Verification for Entitlements Program's user interface will mask the full Social Security Number during data inputs, except for when information is submitted via the bulk uploader. In compliance with the security policy for Social Security numbers, server-side encryption is used for Amazon Simple Storage Service³⁶ and Amazon Relational Database Services³⁷ databases. This uses key management provided by Amazon Web Services for the storage buckets and Relational Database Services databases where Social Security Numbers are housed. Social Security Numbers and Personally Identifiable Information are not exposed in any hard copy documents available for extract from the information system. Additionally, in accordance with the National Institute of Science and Technology and Department of Homeland Security information security and privacy policies, the Systematic Alien Verification for Entitlements Program maintains moderate level controls for the confidentiality of information within the tool.</p>

<p>4. How does the Project, Program, or System retrieve information?</p>	<p><input checked="" type="checkbox"/> By a unique identifier.³⁸ Please list all unique identifiers used:</p> <ul style="list-style-type: none"> • Full name • Alias
---	---

³⁵ See <https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction>.
³⁶ Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. Organizations can use this service to store, manage, analyze, and protect any amount of data for virtually any use case, such as data lakes, cloud-native applications, and mobile apps.
³⁷ Amazon Relational Database Service (Amazon RDS) is an easy-to-manage relational database service optimized for total cost of ownership. It is simple to set up, operate, and scale with demand. Amazon RDS automates undifferentiated database management tasks, such as provisioning, configuring, backing up, and patching. Amazon RDS allows customers to create a new database in minutes and offers flexibility to customize databases to meet their needs.
³⁸ Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 27 of 42

	<ul style="list-style-type: none"> • Date of birth • Immigration enumerator: <ul style="list-style-type: none"> ○ Alien number/United States Citizenship and Immigration Services Number, ○ Form I-94, Arrival/Departure Record number, ○ Student and Exchange Visitor Information System Identification number, ○ Citizenship or Naturalization Certificate number ○ Card Number / I-797 Receipt Number, ○ Visa Number, or ○ Foreign passport number (if submitted with another immigration enumerator) and issuing country • Social Security Number • United States passport number • Customer Agency-issued Case Number • Case Verification Number <p><input type="checkbox"/> By a non-unique identifier or other means. Please describe: <i>Click here to enter text.</i></p>
--	---

<p>5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? If no schedule has been approved, please provide proposed schedule or plans to determine it.</p> <p><i>Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.³⁹</i></p>	<p>Data within Systematic Alien Verification for Entitlements Program is retained for 10 years after the final match determination of the employee or applicant in accordance with NARA approved records retention schedule N1-566-08-07.</p> <p>All United States Citizenship and Immigration Services verification requests will be documented in a transactional database. The retention period is 10 years. The database is not accessible to the public, except as permitted.</p>
--	--

³⁹ See <https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/cdod/rm/Pages/DHS-Records-Officers.aspx>



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 28 of 42

<p>5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)?</p>	<p>Data is automatically purged annually based on NARA disposal schedule NI-566-08-07.</p>
<p>6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?⁴⁰</p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>United States Citizenship and Immigration Services Systems:</p> <ul style="list-style-type: none"> • Central Index System • Electronic Immigration System • Computer Linked Application Information Management System 3 • Enterprise Citizenship and Immigration Services Centralized Operational Repository • GLOBAL (not an acronym) • RAILS (not an acronym) • Customer Profile Management System • Reengineered Naturalization Application Casework System • Marriage Fraud Amendment System • Salesforce Customer Relationship Management Customer Relationship Management⁴¹ <p>Department of Homeland Security Systems:</p> <ul style="list-style-type: none"> • Department of Homeland Security OneNet • Immigration and Custom Enforcement Student and Exchange Visitor Information System • Immigration and Custom ENFORCE Integrated Database

⁴⁰ PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes.

⁴¹ Provides a unified platform where data from different departments can be accessed and used to improve customer interactions.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 29 of 42

	<ul style="list-style-type: none"> • Customs and Border Protection Arrival and Departure Information System • Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data - USPassportRESTService • Transportation Security Administration Technology Infrastructure Modernization and Vetting and Credentialing System
<p>7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?</p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. If yes, please list:</p> <p>The following are systems/organizations that the Systematic Alien Verification for Entitlements Program collects/shares information to support user agencies' requests:</p> <ul style="list-style-type: none"> • United States Military Entrance Processing Command Integrated Resource System • Department of Education Federal Student Aid Central Processing System • Department of Health and Human Services Centers for Medicare & Medicaid Services • Social Security Administration Numident system • Department of Justice Executive Office for Immigration's Immigration Review Information Exchange System • Department of State Consular Consolidated Database Passport <p>The following are systems/organizations that the Systematic Alien Verification for Entitlements provides information that determine benefit eligibility:</p> <ul style="list-style-type: none"> • Various federal agencies in their role as a user agency



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 30 of 42

	<ul style="list-style-type: none"> • Various state, local, tribal, and territory agencies in their role as a Systematic Alien Verification for Entitlements Program user agency
<p>8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? If applicable, please provide agreement as an attachment.</p>	<p>Existing</p> <p>Please describe applicable information sharing governance in place:</p> <ul style="list-style-type: none"> • Letter of Agreement between United States Citizenship and Immigration Services and Social Security Administration • Information Sharing Agreement between the Department of Homeland Security, United States Citizenship and Immigration Services and the Social Security Administration regarding citizenship • Computer Matching Agreement with Department of Education • Memorandum of Agreements between United States Citizenship and Immigration Services and each individual user agency
<p>9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?</p>	<p><input type="checkbox"/> No. What steps will be taken to develop and maintain the accounting: <i>Click here to enter text.</i></p> <p><input checked="" type="checkbox"/> Yes. In what format is the accounting maintained if appropriate (e.g., disclosures to the Department of Justice Office of Special Counsel, Immigration and Customs Enforcement). Verification Information System also has a transactional log that enables the recreation of accounting of disclosures.</p>
<p>10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:</p>	<p><input type="checkbox"/> Social Media</p> <p><input type="checkbox"/> Advanced analytics⁴²</p> <p><input type="checkbox"/> Live PII data for testing</p>

⁴² The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 31 of 42

	<input checked="" type="checkbox"/> No
11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?⁴³ This does not include subject-based searches.	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i>
11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please elaborate: <i>Click here to enter text.</i>
12. Does the planned effort include any interaction or intervention with human subjects⁴⁴ via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for <u>independent</u> review and approval of this effort. ⁴⁵
13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, <u>in addition</u> to annual privacy training required of all DHS personnel?	<input checked="" type="checkbox"/> No. <input type="checkbox"/> Yes. If yes, please list: <i>Click here to enter text.</i>

⁴³ Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—
 (A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals.
 (B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
 (C) the purpose of the queries, searches, or other analyses is not solely—
 (i) the detection of fraud, waste, or abuse in a government agency or program; or
 (ii) the security of a government computer system.

⁴⁴ Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

⁴⁵ For more information about CAPO and their points of contact, please see: <https://www.dhs.gov/publication/capo> or <https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36>. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
 Page 32 of 42

<p>14. Is there a FIPS 199 determination?⁴⁶</p>	<p><input type="checkbox"/> No.</p> <p><input checked="" type="checkbox"/> Yes. Please indicate the determinations for each of the following:</p> <p>Confidentiality: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Integrity: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p> <p>Availability: <input type="checkbox"/> Low <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> Undefined</p>
---	--

PTA REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE REVIEWER)

Component Privacy Office Reviewer:	Chiquita Jones/LeVar Sykes
Component Privacy Office Senior Reviewer:	Shannon DiMartino
PRIVCATS ID Number:	0019946
Date submitted to Component Privacy Office:	May 5, 2025
Concurrence from other Component Reviewers involved (if applicable):	Catherine Shorten, Customs and Border Protection, concurrence provided 6/5/2025
<p>Component Privacy Office Recommendation: <i>Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.</i></p> <p>The United States Citizenship and Immigration Services submits this updated Privacy Threshold Analysis to document the United States Citizenship and Immigration Services Verification Division and Office of Technology (OIT) changes to the Systematic Alien Verification for Entitlements Program. The United States Citizenship and Immigration Services administers the Systematic Alien Verification for Entitlements Program which is an inter-governmental initiative that provides a web-based service to help</p>	

⁴⁶ FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems. For more information, see <https://www.nist.gov/itl/fips-general-information>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 33 of 42

federal, state, territorial, tribal and local agencies and other governmental entities verify United States citizenship or immigration status/category information of applicants for benefits, licenses, or other authorized purposes.

This Privacy Threshold Analysis documents the following changes to the Systematic Alien Verification for Entitlements Program:

1. Expanded search capabilities to allow approved Systematic Alien Verification for Entitlements Program user agencies to verify United States citizenship information using Social Security Numbers and other non-Department of Homeland Security enumerators.
2. A new Social Security Administration system connection to support verification of citizenship/immigration status.
3. A new bulk uploader/list processor function that allows user agencies to upload lists of benefit applicants.
4. Use of the Voter Registration and Voter List Maintenance Verification functionality.
5. The collection of information from the Department of State's Consular Consolidated Database/American Citizen Record Query system.
6. An integration with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data system.

The United States Citizenship and Immigration Services Privacy Office recommends Privacy Impact Assessment coverage for the Systematic Alien Verification for Entitlements Program to comply with the eGovernment Act of 2002 as it "collects, maintains, or disseminates information that is in an identifiable form." The information collected, used, stored, and/or disseminated by the Systematic Alien Verification for Entitlements Program meets the definition of Personally Identifiable Information ("PII")/Sensitive Personally Identifiable Information ("SPII")⁴⁷ as it "permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether that individual is a United States citizen, legal permanent resident, or a visitor to the United States, or employee or contractor to the Department." Specifically, the Systematic Alien Verification for Entitlements Program involves information from members of the public applying for benefits, licenses, or other authorized purposes which may include (1) United States citizens and legal permanent residents, (2) individuals who are now current United States citizens and legal permanent residents after previously naturalizing or adjusting their status, or (3) individuals who may ultimately naturalize to become United States citizens or adjust their status to receive legal permanent residency in the future. Depending on the eligibility category certain individuals may be eligible to apply for adjustment of status as soon as one (1) year after their initial immigration benefit is granted,⁴⁸ therefore the United States Citizenship and Immigration Services Privacy Office recommends requiring Privacy Impact Assessment coverage for the Systematic Alien Verification for Entitlements Program to ensure all current and future United States

⁴⁷ Personally Identifiable Information (PII) has numerous official definitions, but in general, it is defined as any information that can be used to identify an individual directly or indirectly, such as a name, email address, Social Security Number or IP address. Sensitive PII (SPII) is generally defined as any PII that if lost, stolen, or disclosed without authorization could result in significant harm to an individual.

⁴⁸ For more information on eligibility categories please refer to: <https://www.uscis.gov/green-card/green-card-eligibility-categories>.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 34 of 42

citizens and legal permanent residents have transparency into how the United States Citizenship and Immigration Services may collect, store, use, and share the information they previously provided to the United States Citizenship and Immigration Services.

The Privacy Office's Technology Oversight Branch recommends that the Systematic Alien Verification for Entitlements Program continues to be designated as a privacy sensitive program that requires privacy compliance coverage. The Technology Oversight Branch recommends that with the new updates to the program documented in this Privacy Threshold Analysis the Systematic Alien Verification for Entitlements Program be identified as not in compliance with the Privacy Act of 1974, as amended, or the E-Government Act of 2002. A Privacy Impact Assessment update and a System of Records Notice update should be published prior to the program's changed collection and use of Personally Identifiable Information, including information on natural born United States citizens. Further, the sharing of Personally Identifiable Information with the Social Security Administration should occur after the System of Records Notice has gone through the required 30-day comment period. The following are the Technology Oversight Branch's recommendations for privacy compliance coverage and additional requirements:

Privacy Impact Assessment

- A new Privacy Impact Assessment Update for DHS/USCIS/PIA-006 Systematic Alien Verification for Entitlements Program must be completed before collection and use of additional information. Specifically, these Privacy Impact Assessment updates would include, but are not limited to:
 - The collection of Social Security Numbers and other information from the Social Security Administration regarding United States citizens, including natural born citizens.
 - The change in legal rationale for now collecting and maintaining Social Security Numbers of United States natural born citizens.
 - The collection and use of Passport Numbers from the Department of State via new system connections.
 - The addition of the Voter Registration and Voter List Maintenance Verification process, including how this process may verify the citizenship status of natural born United States citizens.
 - The implementation of the bulk case upload functionality for User Agencies.
 - Additional privacy risks and mitigation strategies regarding notice, consent, and data accuracy.

System of Records Notice

- An update to DHS/USCIS-004 Systematic Alien Verification for Entitlements Program must be completed before the collection and sharing of additional information. Specifically, these System of Records Notice updates would include, but are not limited to changes to the following sections:
 - Purpose: The System of Records Notice does not currently include the verification of voter registration and voter maintenance lists.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 35 of 42

- Categories of Individuals: Currently, USCIS specifically informs the public it only collects information on naturalized or acquired United States citizens. This section must be updated to discuss that information on natural born United States citizens will also be collected.
- Categories of Records: The System of Records Notice currently informs the public that the Systematic Alien Verification for Entitlements Program only collects Social Security Number of immigrants on the United States Citizenship and Immigration Services Form G-845. This section must be updated to cover the expanded collection and use of Social Security Numbers.
- Sources of Records: The System of Records Notice currently doesn't include the Social Security Administration system of records. This section must be updated to reflect all new source systems including the Social Security Administration Numident system.
- DHS/CBP-011 Customs and Border Protection Primary and Secondary Processing (TECS (not an acronym)) National SAR Initiative December 19, 2008 (73 Federal Register 77778)
- STATE-26 Passport Records, March 24, 2015 (80 Federal Register 15653)
- STATE-39 Visa Records, November 8, 2021 (86 Federal Register 61822)
- SSA-60-0058 Master Files of Social Security Number Holders and Social Security Number Applications, February 20, 2025 (90 Federal Register 10025)

The following is a Plan of Action to ensure that the Systematic Alien Verification for Entitlements Program is brought into compliance with all federal statutes, regulations, and Department of Homeland Security policies.

USCIS Privacy's Action Plan for the Systematic Alien Verification for Entitlements Program

The Systematic Alien Verification for Entitlements Program is an inter-governmental initiative that provides a web-based service to help federal, state, territorial, tribal and local agencies and other governmental entities verify United States citizenship or immigration status/category information of applicants for benefits, licenses, or other authorized purposes.

Action Plan

This plan outlines priority actions necessary to advance the goal and objective of ensuring the Systematic Alien Verification for Entitlements Program is compliant with all applicable privacy laws, regulations, and policies. These actions will ensure that the use of technology by United States Citizenship and Immigration Services and the Systematic Alien Verification for Entitlements Program sustains and does not erode privacy protections relating to the collection, use, dissemination, maintenance, and disposal of personal information. These actions include actively working with the Verification Division, Office of Chief Counsel and the Customs and Border Protection Office of Privacy on this Privacy Threshold Analysis and the draft System of Records Notice along with continued collaboration with these stakeholders and others such as the Department of Homeland Security Privacy Office to ensure Systematic Alien Verification for Entitlements Program is in compliance.

Actions to Be Taken



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 36 of 42

To meet these objectives the United States Citizenship and Immigration Services Office of Privacy will complete the following activities:

- Receive United States Citizenship and Immigration Services Chief Privacy Officer adjudication of the initial Systematic Alien Verification for Entitlements Program Privacy Threshold Analysis:
 - Adjudication - Date of Completion: July 2025
- Draft an updated Systematic Alien Verification for Entitlement Program Privacy Impact Assessment meeting all requirements identified above and submit the draft to the Department of Homeland Security Office of Privacy.
 - Initial Draft - Complete
 - Office of Chief Counsel Review – Complete
 - Submission to Department of Homeland Security – Date of Completion: September 2025
 - Publication – Estimated September 2025
- Draft an updated Systematic Alien Verification for Entitlement Program System of Records Notice meeting all requirements identified above and submit the draft to the Department of Homeland Security Office of Privacy.
 - Initial Draft - Complete
 - Office of Chief Counsel Review – Complete
 - Submission to Department of Homeland Security – Date of Completion: September 2025
 - Submission to the Office of Management and Budget and Congress – Estimated September 2025
 - Publication – Estimated September 2025
 - End of 30-day commenting period (and sharing of new routine uses) Estimated October/November 2025
- Draft a Privacy Threshold Analysis documenting the new Systematic Alien Verification for Entitlement Program information sharing agreement between the United States Citizenship and Immigration Services and the Social Security Administration and receive the Chief Privacy Officer's adjudication of the Privacy Threshold Analysis.
 - Estimated Date of Completion: September 2025
- Determine the applicability of the Computer Matching and Privacy Protection Act of 1988 to new or changed aspects of the Systematic Alien Verification for Entitlements Program including the new bulk upload functionality for User Agencies.
 - Hold a discussion regarding the Computer Matching Agreement impacts with representatives from the Department of Homeland Security Privacy Office, United States Citizenship and Immigration Services Office of Chief Counsel and Office of Privacy, and Department of Homeland Security Office of General Council.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
[REDACTED]
www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 37 of 42

- Date of Completion: June 2025
 - Decide on the need for Computer Matching Agreements with user agencies versus the current Memorandum of Agreements in place with each Systematic Alien Verification for Entitlement Program user agency:
 - Date of Completion: July/August 2025

This Privacy Threshold Analysis and Action Plan focuses predominantly on Phases One through Four of the Systematic Alien Verification for Entitlements Program Optimization effort as Phase Five and Phase Six are longer term goals of the optimization effort and are still in the exploratory/planning stage. The United States Citizenship and Immigration Services will update this Privacy Threshold Analysis and Action Plan as needed to support the remaining phases during their development and ensure the Systematic Alien Verification for Entitlements Program is compliant with all applicable laws, regulations, and Department of Homeland Security policies.

The updated Privacy Threshold Analyst should also provide, at a minimum, the following updates:

- New status types that Systematic Alien Verification for Entitlements Program may provide to the user agencies and how any additional verification is completed.
- A discussion about the update to the user memorandum of agreements and the creation of the voter verification specific memorandum of agreements.
- Confirm all responses from the Customs and Border Protection via the use of their USPassportRESTService when matching United States Passport numbers.
- Discuss Customs and Border Protection authority/purpose for collecting United States Passport related photographs and collection of those photographs by the United States Citizenship and Immigration Services.
- A description of how the information received via the integration with the Department of Justice to enable an incarceration/felony related flag will be used internally and if any related information will be sent to the user agencies or the applicants.
- If the Systematic Alien Verification for Entitlements Program will use the existing connection by the E-Verify Program to the USPassportRESTService or will it be a new connection.
- Additional use case information for the Systematic Alien Verification for Entitlements Program use of Department of State information from the USPassportRESTService and the Department of State's Consular Consolidated Database / American Citizen Record Query system.
- Clarification regarding user agency benefit applicants accessing the Systematic Alien Verification for Entitlements Program.
- Additional information regarding notification provided to United States citizens regarding user agencies use of their information.
- What information may be provided to the user agency about the VAWA status of an individual.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 38 of 42

- Discussion of if there could be instances when a natural born United States citizen is unable to be verified based on the data available. Also, if all United States citizens would be able to be verified via the SSA information.
- Confirmation if there are additional responses (besides Lawful Status, No Lawful Status, or Deceased) provided to user agencies now that United States citizens can also be verified.
- A discussion of any updates regarding any new agreements between Department of State and Customs and Border Protection for the sharing and use of United States Passport number information.
- Confirmation of if there is still a connection with the Reengineered Naturalization Application Casework System (which was previously decommissioned) or how information from the previously decommissioned system is still accessed.

PTA ADJUDICATION

(TO BE COMPLETED BY THE COMPONENT PRIVACY OFFICE APPROVER)

Component Privacy Office Approver:	Angela Y. Washington
PTA Approval Date:	September 11, 2025
PTA Expiration Date:	December 11, 2025

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	System If "other" is selected, please describe: <i>Click here to enter text.</i>
Determination:	<input type="checkbox"/> Project, Program, System in compliance with full coverage. <input checked="" type="checkbox"/> Project, Program, System in compliance with interim coverage. <input type="checkbox"/> Project, Program, System in compliance until changes implemented. <input type="checkbox"/> Project, Program, System not in compliance.
PIA:	PIA Update is required. <ul style="list-style-type: none"> • DHS/USCIS/PIA-006 Systematic Alien Verification for Entitlement Program <ul style="list-style-type: none"> ○ This PIA must be updated to document all identified system/programmatic changes.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 [Redacted]
www.dhs.gov/privacy

Privacy Threshold Analysis
Version number: 02-2025
Page 39 of 42

SORN:	<p>SORN update is required.</p> <ul style="list-style-type: none"> • DHS/USCIS-004 Systematic Alien Verification for Entitlements Program, May 27, 2020 (85 FR 31798) <ul style="list-style-type: none"> ○ This SORN must be updated to document all identified changes. • DHS/CBP-011 Customs and Border Protection Primary and Secondary Processing (TECS (not an acronym)) National SAR Initiative December 19, 2008 (73 Federal Register 77778) • STATE-26 Passport Records, March 24, 2015 (80 Federal Register 15653) • STATE-39 Visa Records, November 8, 2021 (86 Federal Register 61822) • SSA-60-0058 Master Files of Social Security Number Holders and Social Security Number Applications, February 20, 2025 (90 Federal Register 10025)
<p>Component Privacy Office Adjudication: <i>Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.</i></p>	
<p>The USCIS Office of Privacy is submitting this Privacy Threshold Analysis (PTA) to document the Systematic Alien Verification for Entitlements (SAVE) Program. The Systematic Alien Verification for Entitlements Program is an intergovernmental initiative using a web-based service to help federal, state, territorial, tribal and local benefit-issuing and licensing agencies and other governmental entities determine the immigration status or United States citizenship of applicants for public benefits, licenses, grants, credentials, background investigations, and other lawful purposes, so only entitled applicants receive them. The Systematic Alien Verification for Entitlements Program verifies immigration status/category and United States citizenship against Department of Homeland Security-accessed records. The Systematic Alien Verification for Entitlements Program is not a database but queries Department of Homeland Security-accessed federal records to provide registered user agencies with a verification response. The Systematic Alien Verification for Entitlements Program does not determine an applicant’s eligibility for a specific benefit or license, as this is the responsibility of the benefit/license granting agency.</p> <p>This Privacy Threshold Analysis is being submitted to document multiple updates and planned updates to the Systematic Alien Verification for Entitlements Program as part of the comprehensive optimization of the Systematic Alien Verification for Entitlements Program to ensure a single, reliable source for verifying immigration status and United States citizenship nationwide. This Privacy Threshold Analysis documents the following key changes: (1) an expanded search capabilities to allow approved Systematic Alien Verification for Entitlements Program user agencies to verify United States citizenship information using Social Security Numbers and other non-Department of Homeland Security enumerators, (2) a new Social Security Administration system connection to support verification of citizenship/immigration status, (3) a new bulk uploader/list processor function that allows user agencies to upload lists of benefit applicants, (4) the use of the Voter Registration and Voter List Maintenance Verification functionality, (5) the collection of information from the Department of State’s Consular Consolidated Database/ American</p>	



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 40 of 42

Citizen Record Query system, and (6) an integration with the Customs and Border Protection TECS (not an acronym) - Travel Documents and Encounter Data system.

After a thorough review of the PTA, the USCIS Office of Privacy continues to designate the Systematic Alien Verification for Entitlements Program as a privacy sensitive system/program requiring both Privacy Impact Assessment (PIA) and System of Records Notice (SORN) coverage as it collects/uses Personally Identifiable Information (PII) as well as Sensitive Personally Identifiable Information (SPII) from members of the public, including legal permanent residents and United States Citizens.

The United States Citizenship and Immigration Services Office of Privacy recommends Privacy Impact Assessment coverage for the Systematic Alien Verification for Entitlements Program to comply with the eGovernment Act of 2002 as it “collects, maintains, or disseminates information that is in an identifiable form.” The information collected, used, stored, and/or disseminated by the Systematic Alien Verification for Entitlements Program meets the definition of Personally Identifiable Information (“PII”)/Sensitive Personally Identifiable Information (“SPII”)⁴⁹ as it “permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether that individual is a United States citizen, legal permanent resident, or a visitor to the United States, or employee or contractor to the Department.” Specifically, the Systematic Alien Verification for Entitlements Program involves information from members of the public applying for benefits, licenses, or other authorized purposes which may include (1) United States citizens and legal permanent residents, (2) individuals who are now current United States citizens and legal permanent residents after previously naturalizing or adjusting their status, or (3) individuals who may ultimately naturalize to become United States citizens or adjust their status to receive legal permanent residency in the future. Depending on the eligibility category certain individuals may be eligible to apply for adjustment of status as soon as one (1) year after their initial immigration benefit is granted,⁵⁰ therefore the United States Citizenship and Immigration Services Office of Privacy recommends requiring Privacy Impact Assessment coverage for the Systematic Alien Verification for Entitlements Program to ensure all current and future United States citizens and legal permanent residents have transparency into how the United States Citizenship and Immigration Services may collect, store, use, and share the information they previously provided to the United States Citizenship and Immigration Services.

Privacy Impact Assessment (PIA) coverage is provided by the following:

- DHS/USCIS/PIA-006 Systematic Alien Verification for Entitlement Program
 - **For the Systematic Alien Verification for Entitlement Program to be in compliance with the eGovernment Act of 2002, this Privacy Impact Assessment must be**

⁴⁹ Personally Identifiable Information (PII) has numerous official definitions, but in general, it is defined as any information that can be used to identify an individual directly or indirectly, such as a name, email address, Social Security Number or IP address. Sensitive PII (SPII) is generally defined as any PII that if lost, stolen, or disclosed without authorization could result in significant harm to an individual.

⁵⁰ For more information on eligibility categories please refer to: <https://www.uscis.gov/green-card/green-card-eligibility-categories>.



updated to reflect the identified system and programmatic changes along with a privacy risk assessment of these changes including but not limited to new collections of data, new populations impacted including natural born US citizens, new system connections, new data sharing, and a new bulk upload/reporting functionality.

System of Records Notice (SORN) coverage is required as the information in the Systematic Alien Verification for Entitlement Program is retrieved by a personal identifier. System of Records Notice coverage is provided by the following:

- DHS/USCIS-004 Systematic Alien Verification for Entitlements Program, May 27, 2020 (85 FR 31798)
 - **For the Systematic Alien Verification for Entitlement Program to be in compliance with the Privacy Act of 1974, this System of Records Notice must be updated to reflect the identified system and programmatic changes including that the System of Records will now include information on natural born United States citizens in addition to naturalized or acquired United States citizens. Updates to the System of Records Notice should include but are not limited to updates in the Purpose, Categories of Individuals, Categories of Records, and the Sources of Records sections.**
- DHS/CBP-011 Customs and Border Protection Primary and Secondary Processing (TECS (not an acronym)) National SAR Initiative December 19, 2008 (73 Federal Register 77778)
- STATE-26 Passport Records, March 24, 2015 (80 Federal Register 15653)
- STATE-39 Visa Records, November 8, 2021 (86 Federal Register 61822)
- SSA-60-0058 Master Files of Social Security Number Holders and Social Security Number Applications, February 20, 2025 (90 Federal Register 10025)

While there are currently published SORNs and PIAs associated with the Systematic Alien Verification for Entitlement Program, these documents do not sufficiently provide coverage for the recently implemented and planned system and programmatic changes documented in this Privacy Threshold Analysis. Therefore, the Systematic Alien Verification for Entitlement Program is not in compliance. An updated Privacy Impact Assessment and an updated System of Records Notice must be published for the Systematic Alien Verification for Entitlement Program to be brought into compliance.

An action plan has been developed to enable the Systematic Alien Verification for Entitlement Program to be brought into compliance with all federal laws, statutes, regulations, and Department of Homeland Security policies. A high-level summary of the action plan is as follows:

- Complete the initial Systematic Alien Verification for Entitlements Program Privacy Threshold Analysis.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

www.dhs.gov/privacy

Privacy Threshold Analysis

Version number: 02-2025

Page 42 of 42

- Publish an updated Systematic Alien Verification for Entitlement Program Privacy Impact Assessment to the Department of Homeland Security Office of Privacy website.
- Publish an updated Systematic Alien Verification for Entitlement Program System of Records Notice in the Federal Register and address any comments received during the 30-day public comment period.
- Complete a Privacy Threshold Analysis documenting the new Systematic Alien Verification for Entitlement Program information sharing agreement between the United States Citizenship and Immigration Services and the Social Security Administration.
- Determine the applicability of the Computer Matching and Privacy Protection Act of 1988 and complete any identified requirements.
- Update the Systematic Alien Verification for Entitlements Program Privacy Threshold Analysis and Action Plan as needed to support the ongoing optimization effort.

The Office of Privacy approves this Privacy Threshold Analysis for 3 months to formally document the current privacy posture of the Systematic Alien Verification for Entitlement Program.

On September 10, 2025, USCIS provided the draft Privacy Impact Assessment and System of Records Notice for the Systematic Alien Verification for Entitlements Program to DHS Privacy. These documents reference the collection, use, maintenance, and sharing of the following:

- Information on natural born United States citizens in addition to naturalized or acquired United States citizens
- Voter registration verification
- Social security numbers, including its truncated format
- Sharing of information with the Social Security Administration.

Interim coverage is provided for three (3) months while the Privacy Impact Assessment and System of Records Notice are being reviewed for approval, signature, and publication by DHS Privacy. This interim coverage is only granted for the programmatic changes documented in the Privacy Impact Assessment and System of Records Notice which are currently pending DHS Privacy review.

Any programmatic changes not included in the scope of this Privacy Threshold Analysis will require an update to the Privacy Threshold Analysis to ensure sufficient privacy risk analysis can be completed and any further compliance documentation update requirements can be identified. Further, any programmatic changes to the Systematic Alien Verification for Entitlements Program not documented in these two privacy compliance documents, will require additional updates to the Privacy Impact Assessment and System of Records Notice to be completed and submitted to DHS Privacy prior to receiving interim coverage.

Exhibit 16

DEPARTMENT OF HOMELAND SECURITY (DHS) PRIVACY OFFICE

NARRATIVE STATEMENT

PROPOSAL TO PUBLISH AN UPDATE TO A SYSTEM OF RECORDS

**DHS/USCIS-004 SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENTS (SAVE)
PROGRAM SYSTEM OF RECORDS**

Purpose: The purpose of this system is to provide a service (fee-based for federal agencies) that assists federal, state, territorial, tribal, and local benefit-granting agencies, licensing bureaus, and other authorized entities for any legally mandated purpose in accordance with an authorizing statute to verify the U.S. citizenship and immigration status of individuals, to include naturalized, derived, and U.S. citizens by birth, within their jurisdiction applying for benefits, and to otherwise efficiently administer their programs, to the extent that such disclosure is necessary to enable these agencies and entities to make decisions related to (1) determining eligibility for a federal, state, territorial, tribal, or local public benefit; (2) issuing a license or grant; (3) issuing a government credential; (4) conducting a background investigation; (5) voter verification or (6) any other lawful purpose. This system is also used for the Department of Homeland Security (DHS)/U.S. Citizenship and Immigration Services (USCIS) bond management purposes under section 213 of the Immigration and Nationality Act.

Authority: Authority for having a system for verification of citizenship and immigration status is found in Immigration and Nationality Act, Pub. L. 82-414, 66 Stat. 163 (June 27, 1952), as amended, Immigration Reform and Control Act, Pub. L. 99-603, 100 Stat. 3359 (Nov. 6, 1986); Personal Responsibility and Work Opportunity Reconciliation Act, Pub. L. 104-193, 110 Stat. 2105 (Aug. 22, 1996); Illegal Immigration Reform and Immigrant Responsibility Act, Pub. L. 104-208, 110 Stat. 3009 (Sept. 30, 1996); (8 U.S.C 1373(c)); the REAL ID Act of 2005, Pub. L. 109-13, 119 Stat. 231 (May 11, 2005); Patient Protection and Affordable Care Act, Pub. L. 111-148, 124 Stat. 119 (Mar. 23, 2010), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. 111-152, 124 Stat. 1029 (Mar. 30, 2010); and the Federal Aviation Administration (FAA)-Extension, Safety, and Security Act of 2016, Pub. L. 114-190, 130 Stat. 615 (July 15, 2016), 8 CFR Part 213a (Affidavits of Support on Behalf of Immigrants).

Effect on Individual Privacy: DHS/USCIS evaluated the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system and determined that it has a **major** impact on individual privacy that is outweighed by DHS's interest in assisting federal, state, territorial, tribal, and local benefit-granting agencies, licensing bureaus, and other authorized entities to verify the U.S. citizenship and immigration status of individuals, to include naturalized, derived, and U.S. citizens by birth, within their jurisdiction applying for benefits, and to otherwise efficiently administer their programs. DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program assists DHS/USCIS in meeting its statutory obligation to administer SAVE. DHS/USCIS must collect personally identifiable information to meet this statutory requirement because the data collected from the user agency must be verified against data collected by DHS, USCIS, and other federal agencies to verify citizenship and/or immigration status.

Additionally, DHS/USCIS evaluated several privacy risks related to transparency/notice and

individual participation. The following are examples of the privacy risks and mitigations documented in the related updated SAVE Program Privacy Impact Assessment:

There is a **privacy risk** that all United States citizens, including natural born U.S. citizens, have not been provided notice that the SAVE collects or maintains their information for citizenship and immigration status.

DHS/USCIS **partially mitigates** this risk. It is the responsibility of each registered agency to provide notice to individuals within their jurisdiction of their use of information and sharing with DHS/USCIS. DHS/USCIS is publishing this privacy impact assessment and related System of Records Notice to provide transparency regarding the new categories of information collected and shared to assist registered agencies in verifying citizenship and immigration status of individuals applying for a benefit or license and voter registration verification. The SAVE Program's "Register an Agency for SAVE" explains how an eligible agency can create a memorandum of agreement with the DHS/USCIS. These agreements require registered user agencies to comply with the Privacy Act of 1974, 5 U.S.C. § 552a, as amended, and other applicable laws, regulations, and policies. These policies include transparency and notice to individuals regarding agencies collection and use of personally identifiable information.

There is a **privacy risk** that the new category individuals covered by this assessment/notice, specifically natural born United States citizens, do not have the opportunity to individually participate or consent in how DHS/USCIS uses their information.

DHS/USCIS **cannot mitigate** this risk. Each user agency is responsible for complying with federal and local authorities. DHS/USCIS assumes that each user agency factors in the principles of notice, individual participation, and consent prior to providing information to DHS/USCIS. DHS/USCIS only uses the information for the authorized purpose(s). Individuals should consult their local government agencies to determine the appropriate opt-in or opt-out statute, regulations and policies.

There is a **privacy risk** that the DHS/USCIS may share inaccurate information with registered agencies, which could in turn impact a registered user agency's eligibility determination for an individual.

DHS/USCIS **partially mitigates** this risk. Generally, SAVE has a 3-step process. The first step is a general query of the system. However, due to misspellings of names, transposed numbers, or incomplete information, SAVE may produce inaccurate results. To mitigate this, SAVE has a manual step process where a DHS/USCIS staff member will try to reconcile the request manually. The third step is for DHS/USCIS to get additional documentation from the registered agency. However, this only partially mitigates the risk since the new request using Social Security numbers does not allow for a second and third step review. DHS/USCIS does not have direct access to the Social Security Administration system to support these additional steps. Additionally, registered agencies may not go through all steps to ensure accuracy of information.

There is a **privacy risk** that the DHS/USCIS may use the information it obtains from registered agencies, the Social Security Administration, and the Department of State, for purposes not

authorized by statute or for which it was originally collected.

DHS/USCIS **mitigates this risk** by only collecting information as authorized by the Immigration and Naturalization Act and other authorities mentioned in the Privacy Impact Assessment. The purpose for sharing Social Security numbers with the Social Security Administration and receiving information is to allow user agencies to verify the citizenship or immigration status of individuals applying for a benefit, license, or voter registration verification. The purpose for sharing and receiving U.S. passport information with the Department of State is to verify the citizenship or immigration status of individuals applying for a benefit, license or for voter registration verification. DHS/USCIS will not use the information for any other purposes than to facilitate verification of status to user agencies or to report potential fraud. The Immigration Reform and Control Act (ICRA) of 1986 Section 121 (c)(1) specifically mentions that the program is not to be used for administrative (non-criminal) enforcement. Also, each registered agency must execute a memorandum of agreement or computer matching agreement with DHS/USCIS that includes terms that the SAVE will be used in accordance with the law.

Risk of Unauthorized Access: Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need-to-know the information for the performance of their official duties and who have appropriate clearances or permissions.

Compatibility of Routine Uses: The Department of Homeland Security Privacy Office has reviewed the routine uses in this proposed system of records notice and found all of them to be compatible with the purpose of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program. In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

Routine Use:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof
2. Any employee or former employee of DHS in his/her official capacity,
3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee, or
4. The United States or any agency thereof.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to the Department of Justice (DOJ) and other federal agencies when DHS determines that the use of those records is relevant and necessary for the conduct of litigation or other legal proceedings for which DHS or DOJ is a party to the litigation or has a vested interest in the litigation .

Routine Use:

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records in response to congressional requests made on behalf of the individual on which the record is maintained.

Routine Use:

C. To the National Archives and Records Administration (NARA) or General Services Administration (GSA) pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to the National Archives and Records Administration (NARA) or General Services Administration (GSA) to facilitate the inspection of records. This ensures that records are being maintained in a manner consistent with established retention schedules.

Routine Use:

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to facilitate legally authorized audits and oversight operations, and ensure that records are being maintained in accordance with established retention policies and procedures.

Routine Use:

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to agencies, entities, and persons to assist in the response to a suspected or confirmed breach. The sharing of information allows DHS to mitigate, remedy, and respond to the impacts of the suspected or confirmed breach.

Routine Use:

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to assist the recipient agency or entity in responding to a suspected or confirmed breach or preventing, minimizing, or remedying the risk of harm to individuals.

Routine Use:

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to federal, state, local, and other government agencies, as well as international and foreign law enforcement agencies to investigate and prosecute violations or potential violations of law.

Routine Use:

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to contractors and others performing work on behalf of the department to facilitate the completion of department-related functions.

Routine Use:

I. To approved federal, state, tribal, and local government agencies for any legally mandated purpose in accordance with their authorizing statute or law and when an approved Memorandum of Agreement or Computer Matching Agreement is in place between DHS and the entity.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to approved federal, state, tribal, and local government agencies for any legally mandated purpose in accordance with their authorizing statute or law and when an approved Memorandum of Agreement or Computer Matching Agreement is in place between DHS and the entity. This routine use is compatible because it assists in the administration of an approved Memorandum of Agreement or Computer Matching Agreement that is in place between DHS and the entity.

Routine Use:

J. To a federal, state, tribal, or local government agency that oversees or administers federal means-tested public benefits for purposes of seeking reimbursement from sponsors for the value of benefits provided to sponsored applicants, as well as reporting on overall sponsor deeming and reimbursement efforts to appropriate administrative and oversight agencies.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to a federal, state, tribal, or local government agency that oversees or administers federal means-tested public benefits for purposes of seeking reimbursement from sponsors for the value of benefits provided to sponsored applicants, as well as reporting on overall sponsor deeming and reimbursement efforts to appropriate administrative and oversight agencies. This routine use is compatible because it assists in the administration and enforcement of immigration laws.

Routine Use:

K. To airport operators to determine the eligibility of individuals seeking unescorted access to any Security Identification Display Area of an airport, as required by the FAA Extension, Safety, and Security Act of 2016.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to airport operators to determine the eligibility of individuals seeking unescorted access to any Security Identification Display Area of an airport. This routine use is compatible because it assists in the administration and enforcement of immigration laws and ensuring public and national safety.

Routine Use:

L. To the Social Security Administration and other federal, state, tribal, territorial, local, governments and other authorized entities to support U.S. citizenship and immigration status verification when a DHS approved agreement is in place between DHS and the entity.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to federal, state, tribal, territorial, local governments and other authorized entities to help verify U.S. citizenship and immigration status of benefit applicants and voter registrations. The routine use is compatible because it is necessary to enable user agencies to make decisions related to (1) determining eligibility for a federal, state, territorial, tribal, or local public benefit; (2) issuing a license or grant; (3) issuing a government credential; (4) conducting a background investigation; (5) voter verification or (6) any other lawful purpose.

Routine Use:

M. To federal, state, territorial, tribal, local, and other entities that have a legal authority to provide oversight of programs and benefits supported by SAVE for auditing of program requirements and when a DHS-approved agreement (e.g. Memorandum of Agreement (MOA) or Computer Matching Agreement (CMA)) is in place between DHS and the entity. The routine use is compatible because it enables USCIS to assist user agencies to efficiently administer their programs.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to entities with a legal authority to audit or oversee the SAVE case verification records created by other user agencies to ensure compliance with program or benefits U.S. citizenship and immigration status eligibility requirements.

Routine Use:

N. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

Compatibility Analysis:

This routine use allows DHS to disclose records maintained as part of the DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program system of records to the news media and the public in order to preserve the confidence of the public in the DHS, and to demonstrate the accountability of the department, its officers and employees, especially when the records pertaining to individual's U.S. citizenship and immigration status are outweighed by the public interest's in shedding light on DHS/USCIS ability to ensure and enhance SAVE.

Applicable OMB Control Numbers:

Form	Form Name	OMB Control #	Expiration Date
G-845	Verification Request	1615-0101	8/31/2028

List of Changes:

1. Clarifies and informs the public that SAVE has removed transaction charges for all state, local, tribal, and territorial government agencies that use the system. Federal agencies are still charged a fee to use SAVE.
2. Adds individuals that are U.S. citizens by birth to the categories of individuals covered by the system.
3. Updates the categories of records in the system to include collecting both full and truncated (last four digits) Social Security number (other than those collected on Form G-845, *Verification Request*), U.S. passport number, driver's license number, and information from the Social Security Administration.
4. Revises the record source categories to add SSA-60-0058 Master Files of Social Security Number Holders and Social Security Number Applications, February 20, 2025 (90 Fed. Reg. 10025), and state or other national agencies that issue or maintain driver's license information.
5. Amends the routine uses section of the System of Records Notice (SORN) to include adding Routine Use L, sharing with Social Security Administration and other federal organizations; and Routine Use M, to support sharing with federal agencies (e.g. the Department of Health and Human Services) to support auditing of federal programs administered by state, local, and tribal governments (e.g. Medicaid).
6. Includes non-substantive changes, including reorganizing of categories of records, change in the use of terms such as from "derived" citizen/citizenship to "acquired" citizen/citizenship, and spelling out of form names from the previously published notice.

Exhibit 17

UNITED STATES GOVERNMENT
 GENERAL TERMS & CONDITIONS (GT & C)
 FS Form 7600A



Agreement Between Federal Program Agencies for Intragovernmental Reimbursable, Buy/Sell Activity. In accordance with TFM Volume 1, Part 2, Chapter 4700, Appendix 8.

https://www.fiscal.treasury.gov/fsservices/gov/acctg/g_invoice/g_invoice_home.htm

NEW OR MODIFIED GT & C			
General Terms and Conditions (GT&C) Number		GT&C Number:A2505-070-028-078576	
		Requesting Agency (Buyer)	Servicing Agency (Seller)
		Agency Agreement Tracking Number:CI SIRWA25065	Agency Agreement Tracking Number:RAFDHS250004
		Modification Number:0	
		Status:Open	
AGENCY INFORMATION			
1.		Requesting Agency (Buyer)	Servicing Agency (Seller)
	Agency Name	Department of Homeland Security (DHS) United States Citizenship & Immigration Services (USCIS)	Social Security Administration
	Group Name	SAVE Program	DCRDP ODEPPIN RA
	Group Description	5900 Capital Gateway Drive, Camp Springs, MD 20588	Office of Data Exchange, Policy Publications, & International Negotiation Reimbursable Agreements
	Document Inheritance Indicator	Yes	Yes
	Agency Location Code (ALC)	70011512	28040001
	ALC Description	70011512 - 070 - Department of Homeland Security - CITIZENSHIP & IMMIGRATION SVCS	28040001 - 028 - SOCIAL SECURITY ADMINISTRATION - HQ - DIV. OF CENTRAL ACCTING OPERATIONS
	Subordinate Group		DCRDP OISP RA - Office of Income Security Programs Reimbursable Agreements
	Cost Center	07-20-0600-00-00-00-00	
	Business Unit	Headquarters	
Department ID	VER		
GT&C INFORMATION			

2.	GT&C Title	Citizenship and Immigration Status Verification Services	
3.	Business Application	Standard Order Processing	
4.	Order Originating Partner Indicator	Requesting Agency	
5.	Agreement Period	Start Date: 05/15/2025	End Date: 09/30/2025
6.	Termination Days	30	
7.	Agreement Type	Multiple	
8.	Advance Payment Indicator	Are Advance Payments allowed for GT&C? No *If "Yes", the Servicing Agency Advance Payment Authority Title and Citation are required upon creation of an Order against this GT&C.	
9.	Assisted Acquisition Indicator	Will this GT&C accommodate Assisted Acquisitions? No *If "Yes", the Servicing Agency provides acquisition support in awarding and managing contracts on behalf of the Requesting Agency's requirements for products or services. Lines 17 & 18 below for additional detail.	
ESTIMATED AGREEMENT AMOUNT			
10.	Total Direct Cost Amount	\$196,397.17	
	Total Overhead Fees and Charges Amount	\$0.00	
	Total Estimated Amount	\$196,397.17	
	Enforce Total Remaining Amount	Should G-Invoicing enforce the total value of orders to remain below the Total Amount on the GT&C? Yes *If "Yes", G-Invoicing will not allow Order total to exceed the GT&C total.	
ADDITIONAL AGREEMENT INFORMATION			
11.	Explanation of Overhead Fees and Charges		
12.	Requesting Scope		
13.	Requesting Roles		
14.	Servicing Roles	Refer to Information Sharing Letter Agreement.	
15.	Restrictions		
16.	Assisted Acquisitions Small Business Credit Clause	The Servicing Agency will allocate the socio-economic credit to the Requesting Agency for any contract actions it has executed on behalf of the Requesting Agency.	
17.	Disputes	Disputes related to this IAA shall be resolved in accordance with instructions provided in the Treasury Financial Manual (TFM) Volume I, Part 2, Chapter 4700, Appendix 5; Intragovernmental Transaction (IGT) Guide, at http://tfm.fiscal.treasury.gov/content/tfm/v1/p2/c470.html .	
18.	Requesting Assisted Acquisitions		
19.	Servicing Assisted Acquisitions		
20.	Requesting Clauses		

21.	Servicing Clauses	The estimated cost set forth in this agreement is based upon SSA's rough order of magnitude cost estimate to perform systems development work for this effort and is based on an estimated 40 million transactions. Within G-Invoicing, SSA may use G-Invoicing Representative Approvers to ministerially approve agreements (GT&C and Orders). Please refer to the Approved PDF Agreement in the attachment section of this GT&C and any underlying Orders for SSA's official approval.	
22.	Intentionally left blank		
23.	Intentionally left blank		
CLOSE GT&C			
24.			
REJECT GT&C			
25.			
PREPARER INFORMATION			
26.	Preparer Name	Anastasia Collins	
	Preparer Phone	4109655413	
	Preparer Email	anastasia.collins@ssa.gov	
AGREEMENT APPROVALS			
By signing this agreement, you authorize the General Terms and Conditions as stated, and that the scope of the work can be fulfilled. By signing, you agree to periodically review the terms and conditions of the agreement and make any necessary modifications to the GT&C and any affected Order(s)			
		Requesting Initial Approval (required)	Servicing Initial Approval (required)
27.	Name	KAREN TYLER	Jamillah Jackson
	Signature	Electronic Approval On File	Electronic Approval On File
	Title	MPA (b)(6)	Representative Approver on behalf of Jessica Burns MacBride
	Email		jamillah.n.jackson@ssa.gov
	Phone		4109653747
	Fax		
	Date Signed	07/29/2025	07/30/2025
		Requesting Final Approval (required)	Servicing Final Approval (required)
28.	Name	NICOLE WALKER	Jamillah Jackson
	Signature	Electronic Approval On File	Electronic Approval On File
	Title	Acting Budget Officer (b)(6)	Representative Approver on behalf of Jessica Burns MacBride
	Email		jamillah.n.jackson@ssa.gov
	Phone		4109653747
	Fax		
	Date Signed	07/29/2025	07/30/2025

ATTACHMENTS			
Name	File Alias	Updated By	Date/Time
SSA Signed RAFDH S_25000 4_7600 A orc3a.pdf		Collins, Anastasia (S)	08/28/2025 07:55 AM
Legal Agreement USCIS SSA 5-15-25 fe.pdf		Collins, Anastasia (S)	06/24/2025 01:19 PM
SOW - SSA_D. AkpanO CC0708 2025 SSA cmts 7.31.25 final tracked. docx		RAY, KALISHA (R)	08/11/2025 01:30 PM
VER250 028.pdf		RAY, KALISHA (R)	08/04/2025 10:21 AM

UNITED STATES GOVERNMENT
ORDER FORM
FS FORM 7600B



Agreement Between Federal Program Agencies for Intragovernmental Reimbursable, Buy/Sell Activity.
In accordance with TFM Volume 1, Part 2, Chapter 4700, Appendix 8.

<https://www.fiscal.treasury.gov/g-invoice>

G-Invoicing Required Fields have an (*)

NEW OR MODIFIED ORDER			
1.	* Order Number	Order Number: O2508-070-028-115617	
		Order Modification Number: 0	
2.	Order Status	Open	
3.	* General Terms & Conditions (GT&C) Number	A2505-070-028-078576	
4.	* Order Create Date	08/08/2025	
PARTNER INFORMATION			
5.	* Assisted Acquisition Indicator	No	
6.	* Period of Performance	Start Date: 05/15/2025	End Date: 09/30/2025
		Requesting Agency (Buyer)	Servicing Agency (Seller)
7.	* Agency Location Code (ALC)	70011512	28040001
8.	* Agency Name	Department of Homeland Security - CITIZENSHIP & IMMIGRATION SVCS	SOCIAL SECURITY ADMINISTRATION - HQ - DIV. OF CENTRAL ACCTING OPERATIONS
9.	Group Name	SAVE Program	DCRDP ODEPPIN RA
10.	Cost Center	07-20-0600-00-00-00-00	
11.	Business Unit	Headquarters	
12.	Department ID	VER	
13.	Order Tracking Number	CISIRWA25065	RAFDHS250004
14.	Unique Entity ID	R76CSFHNTQK5	
15.	Funding Office Code (Buyer Only)		
16.	Funding Agency Code (Buyer Only)		

17.	Comments		<p>The estimated cost set forth in this agreement is based upon SSA's rough order of magnitude cost estimate to perform systems development work for this effort and is based on an estimated 40 million transactions.</p> <p>Within G-Invoicing, SSA may use Representative Approvers to ministerially approve agreements. Please refer to the Approved PDF Agreement in the attachment section of this Order for SSA's official approval.</p>
-----	----------	--	---

AUTHORITY INFORMATION

18.	* Statutory Authority Fund Type Code	Economy Act	
19.	Statutory Authority Fund Type Title		
20.	Statutory Authority Fund Type Citation		
		Requesting Agency (Buyer)	Servicing Agency (Seller)
21.	Program Authority Title		Section 1106(b) of the Social Security Act
22.	Program Authority Citation		Social Security Act, 42 U.S.C. § 1306

ADVANCE INFORMATION

(Required by Servicing Agency if there is an advance.)

23.	Advance Revenue Recognition Methodology		
24.	Advance Revenue Recognition Description (required if "Other")		
25.	Advance Payment Authority Title		
26.	Advance Payment Authority Citation		
27.	Total Advance Amount		

DELIVERY INFORMATION

(Requesting Agency completes this section.)

28.	* FOB Point	Source/Origin	
29.	Constructive Receipt Days		
30.	Acceptance Point	Source/Origin	
31.	Place of Acceptance		
32.	Inspection Point		

33.	Place of Inspection	
ORDER BILLING		
(Servicing Agency completes this section.)		
34.	*Billing Frequency	Quarterly
35.	Billing Frequency Explanation	
ORDER BILLING		
(Requesting Agency completes this section.)		
36.	Priority Order Indicator	No
37.	Capital Planning and Investment control (CPIC)	No
LINE ITEM		
L1	*Line Number	1
L1	Order Line Status	Active
L1	*Item Code	9999
L1	*Item Description	verification of citizenship information.
L1	*Line Costs Unit of Measure (UOM)	DO
L1	*Unit of Measure Description	Dollars, U.S.
L1	Total Line Costs	\$196,397.17
L1	Order Line Advance Amount	
L1	Product/Service Identifier	
L1	*Capitalized Asset Indicator	False
L1	Item UID Required Indicator	No
L1	*Type of Service Requirements	Severable
SCHEDULE SUMMARY		
L1	S1 *Schedule Number	1
L1	S1 Advance Pay Indicator	No
L1	S1 *Cancel Status (schedule)	Active
L1	S1 *Schedule Unit Cost/Price	\$1.00
L1	S1 *Order Schedule Quantity	196,397.17
L1	S1 Order Schedule Amount	\$196,397.17

SCHEDULE FUNDING INFORMATION																			
			Requesting Agency (Buyer)								Servicing Agency (Seller)								
L1	S1	*Agency TAS	SP	ATA	AID	BPOA	EPOA	A	MAIN	SUB	SP	ATA	AID	BPOA	EPOA	A	MAIN	SUB	
					070			X	5088	000			028	2025	2025		8704	000	
L1	S1	*Agency Business Event Type Code	DISNGF								COLL								
L1	S1	Object Class Code	25.3								11.1								
L1	S1	Additional Accounting Classification	CISIRWA25065																
L1	S1	*Description of Products and/or Services including Bona Fide Need for this order (Buyer Only)	verification of citizenship information.																

SLOA INFORMATION																			
*To capture Agency Internal Accounting																			
			Requesting Agency (Buyer)								Servicing Agency (Seller)								
L1	S1	Accounting Classification Reference Number																	
L1	S1	Reimbursable Flag									Reimbursable								
L1	S1	Federal Award Identifier Number (FAIN)																	
L1	S1	Unique Record Identifier (URI)																	
L1	S1	Activity Address																	
L1	S1	Budget Line Item																	
L1	S1	Budget Fiscal Year									2025								
L1	S1	Security Cooperation (FMS)																	
L1	S1	Security Cooperation Implementing Agency Code																	
L1	S1	Security Cooperation Case Line Item Identifier																	
L1	S1	Sub-Allocation																	
L1	S1	Agency Accounting Identifier																	
L1	S1	Funding Center Identifier									4008048								
L1	S1	Cost Center Identifier																	
L1	S1	Project Identifier																	
L1	S1	Activity Identifier									6163								

L1	S1	Disbursing Identifier	
L1	S1	Cost Element Code	
L1	S1	Work Order Number	
L1	S1	Functional Area	
L1	S1	Agency Security Cooperation Case Designator	
L1	S1	Parent Award Identifier (PAID)	
L1	S1	Procurement Instrument Identifier (PIID)	

SCHEDULE SHIPPING INFORMATION

(Requesting Agency completes this section.)

L1	S1	Ship To Address Identifier	
L1	S1	Ship To Agency Title	
L1	S1	Address 1	
L1	S1	Address 2	
L1	S1	Address 3	
L1	S1	Ship To City	
L1	S1	Ship To Postal Code	
L1	S1	Ship To State	
L1	S1	Ship To Country	
L1	S1	Ship To Location Description	
L1	S1	Delivery/Shipping Information for Product Special Shipping Information	
L1	S1	Delivery/Shipping POC Name	
L1	S1	Delivery/Shipping Information for Product POC Title	
L1	S1	Delivery/Shipping Information for Product POC E-mail Address	
L1	S1	Delivery/Shipping Information for Product POC Telephone Number	

Requesting Agency (Buyer)

Servicing Agency (Seller)

L1	S1	Agency Additional Information		The estimated cost set forth in this agreement is based upon SSA's rough order of magnitude cost estimate to perform systems development work for this effort and is based on an estimated 40 million transactions.
CLOSE ORDER				
38.		Closing Date		
		Closing Comments		
REJECT ORDER				
39.		Reject Date	08/29/2025	
		Reject Comments	Updates to line description, type of service requirements, and bona fide need fields.	
AGENCY POINTS OF CONTACTS (POC)				
		Requesting Agency (Buyer)		Servicing Agency (Seller)
40.	* Agency POC Name	Kalisha Ray	(b)(6)	Anastasia Collins
	* Agency POC E-mail			Anastasia.Collins@ssa.gov
	* Agency POC Phone No			410-965-5413
	Agency POC Fax No			
AGREEMENT APPROVALS				
Funding Official				
The Funds Approving Officials, as identified by the Requesting Agency and Servicing Agency, certify that the funds are accurately cited and can be properly accounted for per the purposes set forth in the Order. The Requesting Agency Funding Official signs to obligate funds. The Servicing Agency Funding Official signs to start the work, and to bill, collect, and properly account for funds from the Requesting Agency, in accordance with the agreement.				
		Requesting Agency (Buyer)		Servicing Agency (Seller)
41.	* Funding Official Name	Chauncey Burrell		Jamillah Jackson
	* Signature	Electronic Approval On File		Electronic Approval On File
	Funding Official Title	Management and Program Analyst (b)(6)		Representative Approver on behalf of Susan Wilschke
	* Funding Official E-mail			jamillah.n.jackson@ssa.gov
	* Funding Official Phone No			4109653747
	Funding Official Fax No			
	Funding Official Date Signed	08/06/2025		09/04/2025
Program Official				
The Program Officials, as identified by the Requesting Agency and Servicing Agency, must ensure that the scope of work is properly defined and can be fulfilled for this order. The Program Official may or may not be the Contracting Officer depending on each agency's IAA business process.				
		Requesting Agency (Buyer)		Servicing Agency (Seller)
42.	* Program Official Name	Chirag Bhavsar		Jamillah Jackson

	* Signature	Electronic Approval On File	Electronic Approval On File
	Program Official Title	Associate Chief of Operations (b)(6)	Representative Approver on behalf of Susan Wilschke
	* Program Official E-mail		jamillah.n.jackson@ssa.gov
	* Program Official Phone No		4109653747
	Program Official Fax No		
	Program Official Date Signed	08/07/2025	09/04/2025

AGENCY PREPARER INFORMATION

		Requesting Agency (Buyer)	Servicing Agency (Seller)
43.	* Name	KALISHA RAY	Anastasia Collins
	* Phone No		4109655413
	* E-mail Address		anastasia.collins@ssa.gov

ATTACHMENTS

Name	File Alias	Uploaded By	Date/Time
SSA Signed RAFDH S_25000 4_7600 B orc3a.pdf		(b)(6)	08/28/2025 08:20 AM



U.S. Citizenship
and Immigration
Services

Statement of Work

1. **Title of Project**

Citizenship and Immigration Status Verification Services

2. **Period of Performance**

05/15/25-09/30/25

3. **Authority**

Reimbursement for activities related to this Statement of Work (SOW) shall be in accordance with the Economy Act, 31 U.S.C. 1535.

DHS-USCIS is authorized to participate in this information sharing under the authority of the Immigration and Nationality Act, Section 103, 8 U.S.C. § 1103, and the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Section 642, codified at 8 U.S.C. § 1373(c).

SSA will provide DHS-USCIS information in accordance with 8 U.S.C. § 1373(a) and 42 U.S.C. § 1306.

This information sharing is also subject to requirements of:

- The Privacy Act of 1974, 5 U.S.C. § 552a;
 - The Federal Information Security Management Act of 2014 (FISMA; Pub. L. 113-283);
 - 20 C.F.R. § 401.120; and
- other laws, rules, regulations and applicable agency policies

4. **Parties**

The parties to this Statement of Work are the U.S. Citizenship and Immigration Services (USCIS) also known as the “Requesting Agency,” and the Social Security Administration (SSA), also known as the “Servicing Agency.”

The Agency Point of Contacts:

5. **USCIS Technical Representative**

Chirag Bhavsar, [redacted] (b)(6)

6. **USCIS Program Manager**

Brian Broderick, [redacted]

7. **SSA Point of Contact:**

Anastasia Collins, Anastasia.collins@ssa.gov, 410-965-5413

8. **Project Background**

SAVE’s citizenship information verification initiative seeks to provide timely



U.S. Citizenship
and Immigration
Services

verification of citizenship or immigration status information in response to voter verification and other authorized inquiries from Federal, State, territorial, tribal and local government agencies seeking to verify or ascertain the citizenship or immigration status of individuals within their jurisdiction by using a social security number, or part thereof, as a search term or method to locate additional information in DHS-USCIS accessed records regarding the individual.

DHS-USCIS seeks access to SSA information accessed through the DHS-USCIS Verification Information System (VIS) for the purpose of verifying the citizenship and immigration status for benefits and licenses, as authorized by section 103 of the Immigration and Nationality Act, Pub. L No. 82-414, as amended, 8 U.S.C. § 1103, Section 121(c)(1), Part C, of the Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 42 U.S.C. § 1320b-7 and note, and section 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, as amended, 8 U.S.C. § 1373(c).

SSA is providing assistance by sending to, and receiving from, DHS-USCIS information regarding the citizenship or immigration status, lawful or unlawful, of individuals within its records.

9. **Scope**

This Statement of Work, the Information Sharing Letter Agreement (dated May 15, 2025), and the applicable financial forms (i.e., FS Forms 7600A and 7600B) constitute the entire Agreement of the Parties with respect to the purposes set forth in this Agreement. SSA and DHS-USCIS have made no representations, warranties, or promises outside of this Agreement for use of data as described in this Agreement. This Agreement takes precedence over any other documents that may be in conflict with it, including any conflicting terms in any Interconnection Security Agreement (“ISA”) entered into in accordance with NIST SP 800-47 governing the interconnection between information technology systems that will be utilized for the transfer of information under this Agreement.

10. **SSA’s Responsibilities**

Under DHS-USCIS’ SAVE process SSA will provide electronic response codes to USCIS’ SAVE queries. These codes report which data elements sent to SSA by SAVE (name, SSN, and date of birth) match data elements in the Master Files of Social Security Number (SSN) Holders and SSN Applications (“Enumeration System”), 60-0058, system of records. The codes also report if there is a death or fraud indicator in the Enumeration System and the person’s citizenship status, as recorded in the Enumeration System.

SSA will provide responses to the SAVE queries within one second or less.

SSA will inform USCIS when its systems have a scheduled outage or planned maintenance that may negatively affect service.



U.S. Citizenship
and Immigration
Services

SSA will safeguard any personally identifiable information (PII) obtained from SAVE agencies through the SAVE process in accordance with FISMA. SSA will limit access to this information to SSA employees involved in resolving SAVE cases, USCIS employees who administer SAVE, and individuals or entities authorized by the U.S. Government to evaluate SAVE.

USCIS' Responsibilities:

USCIS will only submit verification requests to SSA for authorized purposes.

USCIS will notify SSA of any pending or final changes in the statutory or regulatory requirements concerning SAVE.

USCIS will inform SSA if the SAVE system or other related connectivity system has a scheduled outage or planned maintenance that may negatively affect service.

After discovering a connectivity issue that may negatively affect SAVE service, USCIS will inform SSA.

USCIS will safeguard any PII obtained from SSA in accordance with the Privacy Act (5 U.S.C. § 552a) and FISMA. USCIS will limit access to this information to USCIS employees involved in resolving SAVE cases, USCIS employees who administer SAVE, and individuals or entities authorized by the U.S. Government to evaluate SAVE.

11. Security Components

SSA and USCIS will comply with FISMA, 44 U.S.C. § 3551 et seq., as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); FIPS, Mandatory Security Processing Standards 199 & 200; related OMB circulars and memoranda, including revised Circular A- 130, Management of Federal Information Resources (July 28, 2016); National Institute of Standards and Technology (NIST) directives; and the Federal Acquisition Regulations (FAR). These laws, regulations, and directives provide requirements for safeguarding Federal information systems and PII used in Federal agency business processes, as well as related reporting requirements.

FISMA requirements apply to all Federal contractors, organizations, or sources that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Each agency receiving information under this DSA is responsible for oversight and compliance of its contractors and agents with FISMA requirements.

12. Deliverables

SSA will disclose to USCIS data from the Enumeration System, 60-0058, last published in full at 90 Fed. Reg. 10025 (February 20, 2025).

USCIS will maintain information provided by SSA in its system of records entitled,



U.S. Citizenship
and Immigration
Services

“DHS/U.S. Citizenship and Immigration Services (USCIS)-004 Systematic Alien Verification for Entitlements (SAVE) Program System of Records.”

Specified Data Elements

1. SSA will provide SSA with the individual’s name, including other names used as applicable, date of birth, and either the full or partial SSN.

2. SSA will provide USCIS a “verified” or “not verified” response and in the case of a “not verified” response, the reason for the “not verified” will be provided. In rare circumstances, SSA is unable to disclose the reason why an SSN did not verify. In these cases, SSA will provide a reason of “other”.

3. SSA’s responses will contain the following:

- SSN Match (True/False)
- Full SSN for all matches (when a partial SSN is provided)
- Name Match (True/False)
- Date of Birth Match (True/False)
- Citizenship/Foreign Indicator
 - Blank – Citizenship code is blank and foreign-born indicator is blank
 - Citizenship code is blank and foreign-born indicator is *
 - "A" - U.S. Citizen
 - "B" - Legal alien, eligible to work
 - "C" - Legal alien, not eligible to work
 - "D" - Other
 - "E" - Alien Student - restricted work authorized
 - "F" - Conditionally legalized alien
- Alien Registration Number (where applicable)
- Death Indicator (Yes Deceased / Not Deceased)
- Error code descriptions (transaction and record levels)

An applicant for an original SSN provides identifying information, including citizenship, upon application for that number. However, there is no obligation for the SSN holder to report a subsequent change in immigration status to SSA unless that SSN holder files a claim for benefits. Thus, some previously established citizenship information in SSA’s records might not be current. There is no obligation for an individual to report to SSA a change in their citizenship or immigration status until they request a replacement card or file a claim for a Social Security benefit. While the citizenship information is accurate for SSA’s program purposes, if used later for other purposes, it may not be current. SSA is not the custodian of U.S. citizenship records

For individuals whom USCIS provides only a partial SSN, SSA will search our Numident database using USCIS’ supplied names and DOBs, and will only return a response record and full SSN in situations where the alpha search identifies a single individual.



U.S. Citizenship
and Immigration
Services

13. Place of Performance

The performance or delivery by USCIS of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with proper performance of the official duties and obligations of USCIS. If for any reason USCIS delays or fails to provide services, or discontinues the services or any part thereof, USCIS is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

The performance or delivery by SSA of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with the duties described in the Information Sharing Letter Agreement. If for any reason SSA delays or fails to provide services, or discontinues the services or any part thereof, SSA is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

Under DHS-USCIS' SAVE process SSA will provide electronic response codes to USCIS' SAVE queries. These codes report which data elements sent to SSA by SAVE (name, SSN, and date of birth) match data elements in the Enumeration System. The codes also report if there is a death or fraud indicator in the Enumeration System and the person's citizenship status, as recorded in the Enumeration System.

This SOW shall be effective upon the signature of the last signatory hereto and shall continue until the end of the Period of Performance described in Section 2.

14. Billings and Accompanying Documentation

SSA will bill USCIS for services rendered on a quarterly basis using the Treasury G-Invoicing System and collect said charges via Intra-governmental Payment and Collection (IPAC).

Accompanying documentation includes the LETTER AGREEMENT PROVIDING FOR INFORMATION SHARING BETWEEN THE DEPARTMENT OF HOMELAND SECURITY (DHS), U.S. CITIZENSHIP AND IMMIGRATION SERVICES (USCIS) AND THE SOCIAL SECURITY ADMINISTRATION (SSA) REGARDING CITIZENSHIP, and the FS Forms 7600A and 7600B.

15. Modification

Modifications to this Agreement must be in writing and agreed to by the parties.

This Agreement may be terminated by either party upon 30 days advance written notice.

If legislation is enacted that affects SAVE functions or provides for new functionality, the parties agree to modify this Agreement as appropriate to cover any new provisions.

16. Dispute Resolution

Disagreements on the interpretation of the provisions of this SOW that cannot be resolved between USCIS and the SSA point of contact should be provided in writing to the authorized officials at both agencies for resolution. If settlement cannot be reached at



U.S. Citizenship
and Immigration
Services

this level, the disagreement will be elevated to the next level in accordance with DHS-
USCIS procedures for final resolution.

17. Termination

This Agreement may be terminated by either party upon 30 days advance written notice **or**
terminated in accordance with the provisions of this Agreement.

REQUISITION — MATERIALS-SUPPLIES-EQUIPMENT				1. NUMBER VER250028		
SEE INSTRUCTIONS ON REVERSE				2. DATE 21-MAY-2025		
				3. ACTIVITY SYMBOL See Attachment A		
4. TO: NAME AND ADDRESS -- PROCUREMENT SECTION (OR STOREROOM) USCIS BURLINGTON CONTRACTING OFFICE 70 KIMBALL AVE SOUTH BURLINGTON, VT 05403			5. FROM: NAME AND ADDRESS -- REQUISITIONER DHS-USCIS-VERIFICATION DIVISION <div style="border: 1px solid black; width: 150px; height: 20px; margin: 5px 0;"></div> (b)(6) 5900 CAPITAL GATEWAY DRIVE, MAIL STOP 2600 CAMP SPRINGS, MD 20529-0009 US			
6 STOCK NUMBER	7 DESCRIPTION OF ARTICLE (MAKE, MODEL, TYPE, SIZE, COLOR, MFG., ETC)	8 QUANTITY	9 UNIT	10 COST		12 ACTION CODE
				11 UNIT PRICE	11 AMOUNT	
CLIN 0001	INITIAL DEVELOPMENT COSTS AND TRANSACTIONS	1	EA	196,397.17	196,397.17	
<p>Justification: TO FUND THE SOCIAL SECURITY ADMINISTRATION (SSA) SAVE OPTIMIZATION INITIAL DEVELOPMENT COSTS AND QUERIES. PROPOSED POP: 5/23/58-5/22/26</p> <p>Recommended Vendor: No Recommended Vendor</p>						
13. SIGNATURE OF APPROVING OFFICIAL F L OWENS		Date 21-MAY-2025	14. TITLE OF APPROVING OFFICIAL SUPVY MGMT & PROG ANAL			
24. SIGNATURE OF FUNDING OFFICIAL R A COX		Date 21-MAY-2025	25. TITLE OF FUNDING OFFICIAL MGMT & PROG ANAL		15. TOTAL 196,397.17	
16. KEY TO ACTION CODE				PROCUREMENT SECTION (OR STOREROOM)		
S	SUBSTITUTE ITEM	2	CANCELLED--NOT STOCKED	17. DATE RECEIVED		19. PURCHASE ORDER
B	BACK ORDERED	3	CANCELLED--NOT ABLE TO IDENTIFY			DATE
D	PURCHASED FOR DIRECT SHIPMENT	0	OTHER -- AS INDICATED	18. APPROVED		NUMBER
1	CANCELLED--STOCK EXHAUSTED					
I CERTIFY THAT THE ABOVE ARTICLES -- COLUMNS 3, 9 AND 12 - HAVE BEEN RECEIVED.						
20. LOCATION		21. DATE		22. SIGNATURE		23. TITLE

INSTRUCTIONS**Use**

Use Form G-514 - continued on Form G-514.1 -- To requisition materials, supplies, and equipment through the Procurement section of the Regional (or Central) Office; or from a Service-operated Storeroom.

Copies - Distribution

Prepared by requisitioner in an original and two copies, sending original (white) and Copy 1 (pink) to: Procurement Section (or Storeroom), and retaining Copy 2 (green). Procurement Section (or Storeroom) shall, as a rule, pack Copy 1 with shipment, or return it to requisitioner with appropriate advice.

Entries**By requisitioner:**

1. Number consecutively, beginning with number one each fiscal year, and prefix with alphabetic location symbol and last two digits of fiscal year (e.g., MIA-58-1, MIA-58-2, MIA-58-3, etc., MIA-59-1, MIA-59-2, MIA-59-3, etc.). Number continuation sheets with numerical suffix (e.g., MIA-58-1.1, MIA-58-1.2, MIA-58-1.3, etc.).
2. Enter date of preparation.
3. Enter numerical symbol of activity which will benefit from use of articles.
4. Enter name and address of Procurement section (or Storeroom) (e.g., Procurement Section, Immigration and Naturalization Service, Richmond, VA).
5. Enter full name, title, and address so that shipping label may be prepared without reference to address directory. If consignee is other than requisitioner, enter shipping instructions under Entry 7.
6. Enter form numbers; stock number shown in "Stores Stock Catalog" and "Federal Supply Schedules."
7. Enter full description of article; attach sketches, plans, samples, etc. If consignee is other than requisitioner, enter shipping instructions.
8. Enter issue - unit quantity.
9. Enter unit of issue (e.g., each, doz., C, gross, ream, M; lb., cwt, ton; bag, ball, bbl., bot., box, can, pkg., roll, tube; pt., qt., gal., etc.)
13. Signature of approving official.
14. Enter title of approving official.
24. Signature of funding official.
25. Enter title of funding official.

By Procurement Section (or Storeroom):

10. Enter unit price.
11. Enter product of Entries 8 and 10.
12. Enter symbol of action taken. See Entry 16.
15. Enter total of amounts under Entry 11.
17. Enter date requisition received.
18. Signature of approving officer.
19. Enter, if issued, date and number of purchase order.

By consignee:

20. Enter address - city and state.
21. Enter date shipment received.
22. Signature of employee authorized to accept delivery.
23. Enter title of receiving employee.

Form G-514

REQUISITION - MATERIALS-SUPPLIES-EQUIPMENT
Activity Symbols
ATTACHMENT A

REQUISITION NUMBER: VER250028

Item No.	Contract No.	Task Ord No.	Project	Task	Fund	Program	Organization	Object	UOE	Amount
			39ASV01	000	EX	11-04-00-000	07-20-0000-00-00-00	GE25-11-00	0000000	\$196,397.17

APPROPRIATION SYMBOL CROSSWALK:

FUND	FY	TAS	TITLE	AMOUNT
EX	2025	70X5088	Immigration Examination Fees, Immigration Services, Department of Homeland Security	196,397.17

Exhibit 18

UNITED STATES GOVERNMENT
 GENERAL TERMS & CONDITIONS (GT & C)
 FS Form 7600A



Agreement Between Federal Program Agencies for Intragovernmental Reimbursable, Buy/Sell Activity. In accordance with TFM Volume 1, Part 2, Chapter 4700, Appendix 8.

https://www.fiscal.treasury.gov/fsservices/gov/acctg/g_invoice/g_invoice_home.htm

NEW OR MODIFIED GT & C			
General Terms and Conditions (GT&C) Number		GT&C Number:A2505-070-028-078576	
		Requesting Agency (Buyer)	Servicing Agency (Seller)
		Agency Agreement Tracking Number:CI SIRWA25065	Agency Agreement Tracking Number:RAFDHS250004
		Modification Number:0	
		Status:Open	
AGENCY INFORMATION			
1.		Requesting Agency (Buyer)	Servicing Agency (Seller)
	Agency Name	Department of Homeland Security (DHS) United States Citizenship & Immigration Services (USCIS)	Social Security Administration
	Group Name	SAVE Program	DCRDP ODEPPIN RA
	Group Description	5900 Capital Gateway Drive, Camp Springs, MD 20588	Office of Data Exchange, Policy Publications, & International Negotiation Reimbursable Agreements
	Document Inheritance Indicator	Yes	Yes
	Agency Location Code (ALC)	70011512	28040001
	ALC Description	70011512 - 070 - Department of Homeland Security - CITIZENSHIP & IMMIGRATION SVCS	28040001 - 028 - SOCIAL SECURITY ADMINISTRATION - HQ - DIV. OF CENTRAL ACCTING OPERATIONS
	Subordinate Group		DCRDP OISP RA - Office of Income Security Programs Reimbursable Agreements
	Cost Center	07-20-0600-00-00-00-00	
Business Unit	Headquarters		
Department ID	VER		
GT&C INFORMATION			

2.	GT&C Title	Citizenship and Immigration Status Verification Services	
3.	Business Application	Standard Order Processing	
4.	Order Originating Partner Indicator	Requesting Agency	
5.	Agreement Period	Start Date: 05/15/2025	End Date: 09/30/2025
6.	Termination Days	30	
7.	Agreement Type	Multiple	
8.	Advance Payment Indicator	Are Advance Payments allowed for GT&C? No *If "Yes", the Servicing Agency Advance Payment Authority Title and Citation are required upon creation of an Order against this GT&C.	
9.	Assisted Acquisition Indicator	Will this GT&C accommodate Assisted Acquisitions? No *If "Yes", the Servicing Agency provides acquisition support in awarding and managing contracts on behalf of the Requesting Agency's requirements for products or services. Lines 17 & 18 below for additional detail.	
ESTIMATED AGREEMENT AMOUNT			
10.	Total Direct Cost Amount	\$196,397.17	
	Total Overhead Fees and Charges Amount	\$0.00	
	Total Estimated Amount	\$196,397.17	
	Enforce Total Remaining Amount	Should G-Invoicing enforce the total value of orders to remain below the Total Amount on the GT&C? Yes *If "Yes", G-Invoicing will not allow Order total to exceed the GT&C total.	
ADDITIONAL AGREEMENT INFORMATION			
11.	Explanation of Overhead Fees and Charges		
12.	Requesting Scope		
13.	Requesting Roles		
14.	Servicing Roles	Refer to Information Sharing Letter Agreement.	
15.	Restrictions		
16.	Assisted Acquisitions Small Business Credit Clause	The Servicing Agency will allocate the socio-economic credit to the Requesting Agency for any contract actions it has executed on behalf of the Requesting Agency.	
17.	Disputes	Disputes related to this IAA shall be resolved in accordance with instructions provided in the Treasury Financial Manual (TFM) Volume I, Part 2, Chapter 4700, Appendix 5; Intragovernmental Transaction (IGT) Guide, at http://tfm.fiscal.treasury.gov/content/tfm/v1/p2/c470.html .	
18.	Requesting Assisted Acquisitions		
19.	Servicing Assisted Acquisitions		
20.	Requesting Clauses		

21.	Servicing Clauses	The estimated cost set forth in this agreement is based upon SSA's rough order of magnitude cost estimate to perform systems development work for this effort and is based on an estimated 40 million transactions. Within G-Invoicing, SSA may use G-Invoicing Representative Approvers to ministerially approve agreements (GT&C and Orders). Please refer to the Approved PDF Agreement in the attachment section of this GT&C and any underlying Orders for SSA's official approval.	
22.	Intentionally left blank		
23.	Intentionally left blank		
CLOSE GT&C			
24.			
REJECT GT&C			
25.			
PREPARER INFORMATION			
26.	Preparer Name	Anastasia Collins	
	Preparer Phone	4109655413	
	Preparer Email	anastasia.collins@ssa.gov	
AGREEMENT APPROVALS			
By signing this agreement, you authorize the General Terms and Conditions as stated, and that the scope of the work can be fulfilled. By signing, you agree to periodically review the terms and conditions of the agreement and make any necessary modifications to the GT&C and any affected Order(s)			
		Requesting Initial Approval (required)	Servicing Initial Approval (required)
27.	Name	KAREN TYLER	Jamillah Jackson
	Signature	Electronic Approval On File	Electronic Approval On File
	Title	MPA (b)(6)	Representative Approver on behalf of Jessica Burns MacBride
	Email		jamillah.n.jackson@ssa.gov
	Phone		4109653747
	Fax		
	Date Signed	07/29/2025	07/30/2025
		Requesting Final Approval (required)	Servicing Final Approval (required)
28.	Name	NICOLE WALKER	Jamillah Jackson
	Signature	Electronic Approval On File	Electronic Approval On File
	Title	Acting Budget Officer (b)(6)	Representative Approver on behalf of Jessica Burns MacBride
	Email		jamillah.n.jackson@ssa.gov
	Phone		4109653747
	Fax		
	Date Signed	07/29/2025	07/30/2025

ATTACHMENTS			
Name	File Alias	Updated By	Date/Time
SSA Signed RAFDH S_25000 4_7600 A orc3a.pdf		Collins, Anastasia (S)	08/28/2025 07:55 AM
Legal Agreement USCIS SSA 5-15-25 fe.pdf		Collins, Anastasia (S)	06/24/2025 01:19 PM
SOW - SSA_D. AkpanO CC0708 2025 SSA cmts 7.31.25 final tracked. docx		RAY, KALISHA (R)	08/11/2025 01:30 PM
VER250 028.pdf		RAY, KALISHA (R)	08/04/2025 10:21 AM

**UNITED STATES GOVERNMENT
ORDER FORM
FS FORM 7600B**



Agreement Between Federal Program Agencies for Intragovernmental Reimbursable, Buy/Sell Activity.
In accordance with TFM Volume 1, Part 2, Chapter 4700, Appendix 8.

<https://www.fiscal.treasury.gov/g-invoice>

G-Invoicing Required Fields have an (*)

NEW OR MODIFIED ORDER			
1.	* Order Number	Order Number: O2508-070-028-115617	
		Order Modification Number: 0	
2.	Order Status	Open	
3.	* General Terms & Conditions (GT&C) Number	A2505-070-028-078576	
4.	* Order Create Date	08/08/2025	
PARTNER INFORMATION			
5.	* Assisted Acquisition Indicator	No	
6.	* Period of Performance	Start Date: 05/15/2025	End Date: 09/30/2025
		Requesting Agency (Buyer)	Servicing Agency (Seller)
7.	* Agency Location Code (ALC)	70011512	28040001
8.	* Agency Name	Department of Homeland Security - CITIZENSHIP & IMMIGRATION SVCS	SOCIAL SECURITY ADMINISTRATION - HQ - DIV. OF CENTRAL ACCTING OPERATIONS
9.	Group Name	SAVE Program	DCRDP ODEPPIN RA
10.	Cost Center	07-20-0600-00-00-00-00	
11.	Business Unit	Headquarters	
12.	Department ID	VER	
13.	Order Tracking Number	CISIRWA25065	RAFDHS250004
14.	Unique Entity ID	R76CSFHNTQK5	
15.	Funding Office Code (Buyer Only)		
16.	Funding Agency Code (Buyer Only)		

17.	Comments		<p>The estimated cost set forth in this agreement is based upon SSA's rough order of magnitude cost estimate to perform systems development work for this effort and is based on an estimated 40 million transactions.</p> <p>Within G-Invoicing, SSA may use Representative Approvers to ministerially approve agreements. Please refer to the Approved PDF Agreement in the attachment section of this Order for SSA's official approval.</p>
-----	----------	--	---

AUTHORITY INFORMATION

18.	* Statutory Authority Fund Type Code	Economy Act	
19.	Statutory Authority Fund Type Title		
20.	Statutory Authority Fund Type Citation		
		Requesting Agency (Buyer)	Servicing Agency (Seller)
21.	Program Authority Title		Section 1106(b) of the Social Security Act
22.	Program Authority Citation		Social Security Act, 42 U.S.C. § 1306

ADVANCE INFORMATION

(Required by Servicing Agency if there is an advance.)

23.	Advance Revenue Recognition Methodology		
24.	Advance Revenue Recognition Description (required if "Other")		
25.	Advance Payment Authority Title		
26.	Advance Payment Authority Citation		
27.	Total Advance Amount		

DELIVERY INFORMATION

(Requesting Agency completes this section.)

28.	* FOB Point	Source/Origin	
29.	Constructive Receipt Days		
30.	Acceptance Point	Source/Origin	
31.	Place of Acceptance		
32.	Inspection Point		

33.	Place of Inspection	
ORDER BILLING		
(Servicing Agency completes this section.)		
34.	*Billing Frequency	Quarterly
35.	Billing Frequency Explanation	
ORDER BILLING		
(Requesting Agency completes this section.)		
36.	Priority Order Indicator	No
37.	Capital Planning and Investment control (CPIC)	No
LINE ITEM		
L1	*Line Number	1
L1	Order Line Status	Active
L1	*Item Code	9999
L1	*Item Description	verification of citizenship information.
L1	*Line Costs Unit of Measure (UOM)	DO
L1	*Unit of Measure Description	Dollars, U.S.
L1	Total Line Costs	\$196,397.17
L1	Order Line Advance Amount	
L1	Product/Service Identifier	
L1	*Capitalized Asset Indicator	False
L1	Item UID Required Indicator	No
L1	*Type of Service Requirements	Severable
SCHEDULE SUMMARY		
L1	S1 *Schedule Number	1
L1	S1 Advance Pay Indicator	No
L1	S1 *Cancel Status (schedule)	Active
L1	S1 *Schedule Unit Cost/Price	\$1.00
L1	S1 *Order Schedule Quantity	196,397.17
L1	S1 Order Schedule Amount	\$196,397.17

SCHEDULE FUNDING INFORMATION																			
			Requesting Agency (Buyer)							Servicing Agency (Seller)									
L1	S1	*Agency TAS	SP	ATA	AID	BPOA	EPOA	A	MAIN	SUB	SP	ATA	AID	BPOA	EPOA	A	MAIN	SUB	
					070			X	5088	000			028	2025	2025		8704	000	
L1	S1	*Agency Business Event Type Code	DISNGF							COLL									
L1	S1	Object Class Code	25.3							11.1									
L1	S1	Additional Accounting Classification	CISIRWA25065																
L1	S1	*Description of Products and/or Services including Bona Fide Need for this order (Buyer Only)	verification of citizenship information.																

SLOA INFORMATION

*To capture Agency Internal Accounting

			Requesting Agency (Buyer)							Servicing Agency (Seller)									
L1	S1	Accounting Classification Reference Number																	
L1	S1	Reimbursable Flag								Reimbursable									
L1	S1	Federal Award Identifier Number (FAIN)																	
L1	S1	Unique Record Identifier (URI)																	
L1	S1	Activity Address																	
L1	S1	Budget Line Item																	
L1	S1	Budget Fiscal Year								2025									
L1	S1	Security Cooperation (FMS)																	
L1	S1	Security Cooperation Implementing Agency Code																	
L1	S1	Security Cooperation Case Line Item Identifier																	
L1	S1	Sub-Allocation																	
L1	S1	Agency Accounting Identifier																	
L1	S1	Funding Center Identifier								4008048									
L1	S1	Cost Center Identifier																	
L1	S1	Project Identifier																	
L1	S1	Activity Identifier								6163									

L1	S1	Disbursing Identifier	
L1	S1	Cost Element Code	
L1	S1	Work Order Number	
L1	S1	Functional Area	
L1	S1	Agency Security Cooperation Case Designator	
L1	S1	Parent Award Identifier (PAID)	
L1	S1	Procurement Instrument Identifier (PIID)	

SCHEDULE SHIPPING INFORMATION

(Requesting Agency completes this section.)

L1	S1	Ship To Address Identifier	
L1	S1	Ship To Agency Title	
L1	S1	Address 1	
L1	S1	Address 2	
L1	S1	Address 3	
L1	S1	Ship To City	
L1	S1	Ship To Postal Code	
L1	S1	Ship To State	
L1	S1	Ship To Country	
L1	S1	Ship To Location Description	
L1	S1	Delivery/Shipping Information for Product Special Shipping Information	
L1	S1	Delivery/Shipping POC Name	
L1	S1	Delivery/Shipping Information for Product POC Title	
L1	S1	Delivery/Shipping Information for Product POC E-mail Address	
L1	S1	Delivery/Shipping Information for Product POC Telephone Number	
			Requesting Agency (Buyer)
			Servicing Agency (Seller)

L1	S1	Agency Additional Information		The estimated cost set forth in this agreement is based upon SSA's rough order of magnitude cost estimate to perform systems development work for this effort and is based on an estimated 40 million transactions.
CLOSE ORDER				
38.		Closing Date		
		Closing Comments		
REJECT ORDER				
39.		Reject Date	08/29/2025	
		Reject Comments	Updates to line description, type of service requirements, and bona fide need fields.	
AGENCY POINTS OF CONTACTS (POC)				
		Requesting Agency (Buyer)		Servicing Agency (Seller)
40.	* Agency POC Name	Kalisha Ray	(b)(6)	Anastasia Collins
	* Agency POC E-mail			Anastasia.Collins@ssa.gov
	* Agency POC Phone No			410-965-5413
	Agency POC Fax No			
AGREEMENT APPROVALS				
Funding Official				
The Funds Approving Officials, as identified by the Requesting Agency and Servicing Agency, certify that the funds are accurately cited and can be properly accounted for per the purposes set forth in the Order. The Requesting Agency Funding Official signs to obligate funds. The Servicing Agency Funding Official signs to start the work, and to bill, collect, and properly account for funds from the Requesting Agency, in accordance with the agreement.				
		Requesting Agency (Buyer)		Servicing Agency (Seller)
41.	* Funding Official Name	Chauncey Burrell		Jamillah Jackson
	* Signature	Electronic Approval On File		Electronic Approval On File
	Funding Official Title	Management and Program Analyst (b)(6)		Representative Approver on behalf of Susan Wilschke
	* Funding Official E-mail			jamillah.n.jackson@ssa.gov
	* Funding Official Phone No			4109653747
	Funding Official Fax No			
	Funding Official Date Signed	08/06/2025		09/04/2025
Program Official				
The Program Officials, as identified by the Requesting Agency and Servicing Agency, must ensure that the scope of work is properly defined and can be fulfilled for this order. The Program Official may or may not be the Contracting Officer depending on each agency's IAA business process.				
		Requesting Agency (Buyer)		Servicing Agency (Seller)
42.	* Program Official Name	Chirag Bhavsar		Jamillah Jackson

	* Signature	Electronic Approval On File	Electronic Approval On File
	Program Official Title	Associate Chief of Operations (b)(6)	Representative Approver on behalf of Susan Wilschke
	* Program Official E-mail		jamillah.n.jackson@ssa.gov
	* Program Official Phone No		4109653747
	Program Official Fax No		
	Program Official Date Signed	08/07/2025	09/04/2025

AGENCY PREPARER INFORMATION

		Requesting Agency (Buyer)	Servicing Agency (Seller)
43.	* Name	KALISHA RAY	Anastasia Collins
	* Phone No		4109655413
	* E-mail Address		anastasia.collins@ssa.gov

ATTACHMENTS

Name	File Alias	Uploaded By	Date/Time
SSA Signed RAFDH S_25000 4_7600 B orc3a.pdf		(b)(6)	08/28/2025 08:20 AM



U.S. Citizenship and Immigration Services

Statement of Work

1. **Title of Project**

Citizenship and Immigration Status Verification Services

2. **Period of Performance**

05/15/25-09/30/25

3. **Authority**

Reimbursement for activities related to this Statement of Work (SOW) shall be in accordance with the Economy Act, 31 U.S.C. 1535.

DHS-USCIS is authorized to participate in this information sharing under the authority of the Immigration and Nationality Act, Section 103, 8 U.S.C. § 1103, and the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Section 642, codified at 8 U.S.C. § 1373(c).

SSA will provide DHS-USCIS information in accordance with 8 U.S.C. § 1373(a) and 42 U.S.C. § 1306.

This information sharing is also subject to requirements of:

- The Privacy Act of 1974, 5 U.S.C. § 552a;
 - The Federal Information Security Management Act of 2014 (FISMA; Pub. L. 113-283);
 - 20 C.F.R. § 401.120; and
- other laws, rules, regulations and applicable agency policies

4. **Parties**

The parties to this Statement of Work are the U.S. Citizenship and Immigration Services (USCIS) also known as the “Requesting Agency,” and the Social Security Administration (SSA), also known as the “Servicing Agency.”

The Agency Point of Contacts:

5. **USCIS Technical Representative**

Chirag Bhavsar, [redacted] (b)(6)

6. **USCIS Program Manager**

Brian Broderick, [redacted]

7. **SSA Point of Contact:**

Anastasia Collins, Anastasia.collins@ssa.gov, 410-965-5413

8. **Project Background**

SAVE’s citizenship information verification initiative seeks to provide timely



U.S. Citizenship
and Immigration
Services

verification of citizenship or immigration status information in response to voter verification and other authorized inquiries from Federal, State, territorial, tribal and local government agencies seeking to verify or ascertain the citizenship or immigration status of individuals within their jurisdiction by using a social security number, or part thereof, as a search term or method to locate additional information in DHS-USCIS accessed records regarding the individual.

DHS-USCIS seeks access to SSA information accessed through the DHS-USCIS Verification Information System (VIS) for the purpose of verifying the citizenship and immigration status for benefits and licenses, as authorized by section 103 of the Immigration and Nationality Act, Pub. L. No. 82-414, as amended, 8 U.S.C. § 1103, Section 121(c)(1), Part C, of the Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 42 U.S.C. § 1320b-7 and note, and section 642 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, as amended, 8 U.S.C. § 1373(c).

SSA is providing assistance by sending to, and receiving from, DHS-USCIS information regarding the citizenship or immigration status, lawful or unlawful, of individuals within its records.

9. **Scope**

This Statement of Work, the Information Sharing Letter Agreement (dated May 15, 2025), and the applicable financial forms (i.e., FS Forms 7600A and 7600B) constitute the entire Agreement of the Parties with respect to the purposes set forth in this Agreement. SSA and DHS-USCIS have made no representations, warranties, or promises outside of this Agreement for use of data as described in this Agreement. This Agreement takes precedence over any other documents that may be in conflict with it, including any conflicting terms in any Interconnection Security Agreement (“ISA”) entered into in accordance with NIST SP 800-47 governing the interconnection between information technology systems that will be utilized for the transfer of information under this Agreement.

10. **SSA’s Responsibilities**

Under DHS-USCIS’ SAVE process SSA will provide electronic response codes to USCIS’ SAVE queries. These codes report which data elements sent to SSA by SAVE (name, SSN, and date of birth) match data elements in the Master Files of Social Security Number (SSN) Holders and SSN Applications (“Enumeration System”), 60-0058, system of records. The codes also report if there is a death or fraud indicator in the Enumeration System and the person’s citizenship status, as recorded in the Enumeration System.

SSA will provide responses to the SAVE queries within one second or less.

SSA will inform USCIS when its systems have a scheduled outage or planned maintenance that may negatively affect service.



U.S. Citizenship
and Immigration
Services

SSA will safeguard any personally identifiable information (PII) obtained from SAVE agencies through the SAVE process in accordance with FISMA. SSA will limit access to this information to SSA employees involved in resolving SAVE cases, USCIS employees who administer SAVE, and individuals or entities authorized by the U.S. Government to evaluate SAVE.

USCIS' Responsibilities:

USCIS will only submit verification requests to SSA for authorized purposes.

USCIS will notify SSA of any pending or final changes in the statutory or regulatory requirements concerning SAVE.

USCIS will inform SSA if the SAVE system or other related connectivity system has a scheduled outage or planned maintenance that may negatively affect service.

After discovering a connectivity issue that may negatively affect SAVE service, USCIS will inform SSA.

USCIS will safeguard any PII obtained from SSA in accordance with the Privacy Act (5 U.S.C. § 552a) and FISMA. USCIS will limit access to this information to USCIS employees involved in resolving SAVE cases, USCIS employees who administer SAVE, and individuals or entities authorized by the U.S. Government to evaluate SAVE.

11. Security Components

SSA and USCIS will comply with FISMA, 44 U.S.C. § 3551 et seq., as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); FIPS, Mandatory Security Processing Standards 199 & 200; related OMB circulars and memoranda, including revised Circular A- 130, Management of Federal Information Resources (July 28, 2016); National Institute of Standards and Technology (NIST) directives; and the Federal Acquisition Regulations (FAR). These laws, regulations, and directives provide requirements for safeguarding Federal information systems and PII used in Federal agency business processes, as well as related reporting requirements.

FISMA requirements apply to all Federal contractors, organizations, or sources that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Each agency receiving information under this DSA is responsible for oversight and compliance of its contractors and agents with FISMA requirements.

12. Deliverables

SSA will disclose to USCIS data from the Enumeration System, 60-0058, last published in full at 90 Fed. Reg. 10025 (February 20, 2025).

USCIS will maintain information provided by SSA in its system of records entitled,



U.S. Citizenship
and Immigration
Services

“DHS/U.S. Citizenship and Immigration Services (USCIS)-004 Systematic Alien Verification for Entitlements (SAVE) Program System of Records.”

Specified Data Elements

1. SSA will provide SSA with the individual’s name, including other names used as applicable, date of birth, and either the full or partial SSN.

2. SSA will provide USCIS a “verified” or “not verified” response and in the case of a “not verified” response, the reason for the “not verified” will be provided. In rare circumstances, SSA is unable to disclose the reason why an SSN did not verify. In these cases, SSA will provide a reason of “other”.

3. SSA’s responses will contain the following:

- SSN Match (True/False)
- Full SSN for all matches (when a partial SSN is provided)
- Name Match (True/False)
- Date of Birth Match (True/False)
- Citizenship/Foreign Indicator
 - Blank – Citizenship code is blank and foreign-born indicator is blank
 - Citizenship code is blank and foreign-born indicator is *
 - "A" - U.S. Citizen
 - "B" - Legal alien, eligible to work
 - "C" - Legal alien, not eligible to work
 - "D" - Other
 - "E" - Alien Student - restricted work authorized
 - "F" - Conditionally legalized alien
- Alien Registration Number (where applicable)
- Death Indicator (Yes Deceased / Not Deceased)
- Error code descriptions (transaction and record levels)

An applicant for an original SSN provides identifying information, including citizenship, upon application for that number. However, there is no obligation for the SSN holder to report a subsequent change in immigration status to SSA unless that SSN holder files a claim for benefits. Thus, some previously established citizenship information in SSA’s records might not be current. There is no obligation for an individual to report to SSA a change in their citizenship or immigration status until they request a replacement card or file a claim for a Social Security benefit. While the citizenship information is accurate for SSA’s program purposes, if used later for other purposes, it may not be current. SSA is not the custodian of U.S. citizenship records

For individuals whom USCIS provides only a partial SSN, SSA will search our Numident database using USCIS’ supplied names and DOBs, and will only return a response record and full SSN in situations where the alpha search identifies a single individual.



U.S. Citizenship
and Immigration
Services

13. Place of Performance

The performance or delivery by USCIS of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with proper performance of the official duties and obligations of USCIS. If for any reason USCIS delays or fails to provide services, or discontinues the services or any part thereof, USCIS is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

The performance or delivery by SSA of the goods and/or services described herein and the timeliness of said delivery are authorized only to the extent that they are consistent with the duties described in the Information Sharing Letter Agreement. If for any reason SSA delays or fails to provide services, or discontinues the services or any part thereof, SSA is not liable for any damages or loss resulting from such delay or for any such failure or discontinuance.

Under DHS-USCIS' SAVE process SSA will provide electronic response codes to USCIS' SAVE queries. These codes report which data elements sent to SSA by SAVE (name, SSN, and date of birth) match data elements in the Enumeration System. The codes also report if there is a death or fraud indicator in the Enumeration System and the person's citizenship status, as recorded in the Enumeration System.

This SOW shall be effective upon the signature of the last signatory hereto and shall continue until the end of the Period of Performance described in Section 2.

14. Billings and Accompanying Documentation

SSA will bill USCIS for services rendered on a quarterly basis using the Treasury G-Invoicing System and collect said charges via Intra-governmental Payment and Collection (IPAC).

Accompanying documentation includes the LETTER AGREEMENT PROVIDING FOR INFORMATION SHARING BETWEEN THE DEPARTMENT OF HOMELAND SECURITY (DHS), U.S. CITIZENSHIP AND IMMIGRATION SERVICES (USCIS) AND THE SOCIAL SECURITY ADMINISTRATION (SSA) REGARDING CITIZENSHIP, and the FS Forms 7600A and 7600B.

15. Modification

Modifications to this Agreement must be in writing and agreed to by the parties.

This Agreement may be terminated by either party upon 30 days advance written notice.

If legislation is enacted that affects SAVE functions or provides for new functionality, the parties agree to modify this Agreement as appropriate to cover any new provisions.

16. Dispute Resolution

Disagreements on the interpretation of the provisions of this SOW that cannot be resolved between USCIS and the SSA point of contact should be provided in writing to the authorized officials at both agencies for resolution. If settlement cannot be reached at



U.S. Citizenship
and Immigration
Services

this level, the disagreement will be elevated to the next level in accordance with DHS-
USCIS procedures for final resolution.

17. Termination

This Agreement may be terminated by either party upon 30 days advance written notice or
terminated in accordance with the provisions of this Agreement.

REQUISITION — MATERIALS-SUPPLIES-EQUIPMENT				1. NUMBER VER250028		
SEE INSTRUCTIONS ON REVERSE				2. DATE 21-MAY-2025		
				3. ACTIVITY SYMBOL See Attachment A		
4. TO: NAME AND ADDRESS -- PROCUREMENT SECTION (OR STOREROOM) USCIS BURLINGTON CONTRACTING OFFICE 70 KIMBALL AVE SOUTH BURLINGTON, VT 05403			5. FROM: NAME AND ADDRESS -- REQUISITIONER DHS-USCIS-VERIFICATION DIVISION <div style="border: 1px solid black; width: 200px; height: 20px; margin: 5px 0;"></div> (b)(6) 5900 CAPITAL GATEWAY DRIVE, MAIL STOP 2600 CAMP SPRINGS, MD 20529-0009 US			
6 STOCK NUMBER	7 DESCRIPTION OF ARTICLE (MAKE, MODEL, TYPE, SIZE, COLOR, MFG., ETC)	8 QUANTITY	9 UNIT	10 COST		12 ACTION CODE
				10 UNIT PRICE	11 AMOUNT	
CLIN 0001	INITIAL DEVELOPMENT COSTS AND TRANSACTIONS	1	EA	196,397	17	17
<p>Justification: TO FUND THE SOCIAL SECURITY ADMINISTRATION (SSA) SAVE OPTIMIZATION INITIAL DEVELOPMENT COSTS AND QUERIES. PROPOSED POP: 5/23/58-5/22/26</p> <p>Recommended Vendor: No Recommended Vendor</p>						
13. SIGNATURE OF APPROVING OFFICIAL F L OWENS		Date 21-MAY-2025	14. TITLE OF APPROVING OFFICIAL SUPVY MGMT & PROG ANAL			
24. SIGNATURE OF FUNDING OFFICIAL R A COX		Date 21-MAY-2025	25. TITLE OF FUNDING OFFICIAL MGMT & PROG ANAL		15. TOTAL 196,397 17	
16. KEY TO ACTION CODE			PROCUREMENT SECTION (OR STOREROOM)			
S	SUBSTITUTE ITEM	2	CANCELLED--NOT STOCKED	17. DATE RECEIVED		19. PURCHASE ORDER
B	BACK ORDERED	3	CANCELLED--NOT ABLE TO IDENTIFY			DATE
D	PURCHASED FOR DIRECT SHIPMENT	0	OTHER -- AS INDICATED	18. APPROVED		NUMBER
1	CANCELLED--STOCK EXHAUSTED					
I CERTIFY THAT THE ABOVE ARTICLES -- COLUMNS 3, 9 AND 12 - HAVE BEEN RECEIVED.						
20. LOCATION		21. DATE	22. SIGNATURE		23. TITLE	

INSTRUCTIONS**Use**

Use Form G-514 - continued on Form G-514.1 -- To requisition materials, supplies, and equipment through the Procurement section of the Regional (or Central) Office; or from a Service-operated Storeroom.

Copies - Distribution

Prepared by requisitioner in an original and two copies, sending original (white) and Copy 1 (pink) to: Procurement Section (or Storeroom), and retaining Copy 2 (green). Procurement Section (or Storeroom) shall, as a rule, pack Copy 1 with shipment, or return it to requisitioner with appropriate advice.

Entries**By requisitioner:**

1. Number consecutively, beginning with number one each fiscal year, and prefix with alphabetic location symbol and last two digits of fiscal year (e.g., MIA-58-1, MIA-58-2, MIA-58-3, etc., MIA-59-1, MIA-59-2, MIA-59-3, etc.). Number continuation sheets with numerical suffix (e.g., MIA-58-1.1, MIA-58-1.2, MIA-58-1.3, etc.).
2. Enter date of preparation.
3. Enter numerical symbol of activity which will benefit from use of articles.
4. Enter name and address of Procurement section (or Storeroom) (e.g., Procurement Section, Immigration and Naturalization Service, Richmond, VA).
5. Enter full name, title, and address so that shipping label may be prepared without reference to address directory. If consignee is other than requisitioner, enter shipping instructions under Entry 7.
6. Enter form numbers; stock number shown in "Stores Stock Catalog" and "Federal Supply Schedules."
7. Enter full description of article; attach sketches, plans, samples, etc. If consignee is other than requisitioner, enter shipping instructions.
8. Enter issue - unit quantity.
9. Enter unit of issue (e.g., each, doz., C, gross, ream, M; lb., cwt, ton; bag, ball, bbl., bot., box, can, pkg., roll, tube; pt., qt., gal., etc.)
13. Signature of approving official.
14. Enter title of approving official.
24. Signature of funding official.
25. Enter title of funding official.

By Procurement Section (or Storeroom):

10. Enter unit price.
11. Enter product of Entries 8 and 10.
12. Enter symbol of action taken. See Entry 16.
15. Enter total of amounts under Entry 11.
17. Enter date requisition received.
18. Signature of approving officer.
19. Enter, if issued, date and number of purchase order.

By consignee:

20. Enter address - city and state.
21. Enter date shipment received.
22. Signature of employee authorized to accept delivery.
23. Enter title of receiving employee.

Form G-514

REQUISITION - MATERIALS-SUPPLIES-EQUIPMENT
Activity Symbols
ATTACHMENT A

REQUISITION NUMBER: VER250028

Item No.	Contract No.	Task Ord No.	Project	Task	Fund	Program	Organization	Object	UOE	Amount
			39ASV01	000	EX	11-04-00-000	07-20-0000-00-00-00	GE25-11-00	0000000	\$196,397.17

APPROPRIATION SYMBOL CROSSWALK:

FUND	FY	TAS	TITLE	AMOUNT
EX	2025	70X5088	Immigration Examination Fees, Immigration Services, Department of Homeland Security	196,397.17

Exhibit 19



SOCIAL SECURITY
Office of the General Counsel
Office of General Law

July 13, 2023

Sent via email and U.S. Mail

Jon Sherman
Litigation Director & Senior Counsel
Fair Elections Center
1825 K Street NW, Suite 450
Washington D.C. 20006
(Tel.) 202-331-0114
jsherman@fairelectionscenter.org

Re: Application for Records and Testimony of a Social Security Administration (SSA) Employee in a Federal Civil Case, *Mi Familia Vota, et al. v. Adrian Fontes, in his official capacity as Arizona Secretary of State, et al.*, 22-cv-509 et al. (consolidated) (D. AZ)

Dear Mr. Sherman:

You filed an application requesting deposition testimony and supporting documents in this matter from an SSA employee regarding the accuracy and reliability of using SSA databases to verify current U.S. citizenship status. Your case involves two consolidated actions challenging Arizona statutes that implement new citizenship investigation procedures for voter registration applicants and existing registered voters. The procedures require local election officials to compare county voter registration information with data contained in SSA's databases to verify citizenship status and voter eligibility. You allege that doing so will cause naturalized voter registration applicants and registered voters to be erroneously flagged as non-citizens based on old or inaccurate data in SSA databases.

You requested information concerning the frequency SSA databases are updated regarding U.S. citizenship status and the procedures SSA uses to update those databases. You also requested any recent Office of the Inspector General (OIG) report, study, or investigation that includes a review of the accuracy and reliability of U.S. citizenship data or information contained in SSA databases. You stated that you do not seek any internal SSA communications or the underlying data stored in SSA databases. You assert that the information sought from SSA is directly relevant to the claims at issue in your case. This letter constitutes the final decision on your application pursuant to the agency's regulations governing a request for testimony by employees and the production of records and information in legal proceedings. As discussed in further detail below, I am denying your application for testimony but providing information and references to publicly available information about the accuracy of SSA's citizenship status.

Page 2 – Jon Sherman

Further, to the extent you seek nonpublic records or testimony from the Office of the Inspector General, you should direct a request in compliance with 20 C.F.R. Part 403 to: Office of the Inspector General, Social Security Administration, 300 Altmeyer Building, 6401 Security Boulevard, Baltimore, MD 21235-6401. *See* 20 C.F.R. § 403.125.

Citizenship Information in SSA Records

While SSA records provide an indication of citizenship, they do not provide definitive information on U.S. citizenship. The Department of Homeland Security (DHS) is responsible for maintaining current immigration and work authorization status for all noncitizens. Individuals achieve citizenship in various ways. The agency responsible for recording and confirming citizenship status depends on how citizenship was achieved. The responsible agency may be DHS, Department of State, or the States. *See* [SSA - POMS: GN 00303.100 - United States \(U.S.\) Citizenship - 06/05/2018](#). SSA is not the agency responsible for making citizenship determinations. Individuals report their citizenship status to SSA when they apply for a Social Security number (SSN). *See* [SSA - POMS: RM 10210.500 - General Information on Evidence of U.S. Citizenship for a Social Security Number \(SSN\) Card - 07/31/2019](#). SSA did not begin to consistently maintain citizenship information until 1981. *See* [Social Security History \(ssa.gov\)](#) (explaining that SSA requirements regarding citizenship arose in the 1970s). Accordingly, SSA does not have citizenship information for all individuals who have been issued an SSN. Moreover, there is no obligation for an individual to report to SSA a change in their immigration status unless the individual is receiving Social Security payments. *See* [SSA - POMS: GN 00303.001 - Requirement of United States \(U.S.\) Citizenship or Appropriate Alien Status - 06/27/2012](#) and [SSA - POMS: RS 00204.010 - Lawful Presence Payment Provisions - 01/04/2017](#). As such, the citizenship SSA maintains merely represents a snapshot of the individual's citizenship status at the time of their interaction with SSA. SSA's records do not provide definitive information about an individual's citizenship status.

Moreover, we have publicly posted on our website information about the accuracy and reliability of the citizenship data that we maintain in the limited data exchanges in which we provide this information, such as:

- Section VI of [Model State Computer Matching and Privacy Protection Act Agreement](#): Individuals applying for SSNs report their citizenship status at the time they apply for their SSNs. There is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files for a Social Security benefit. State Agencies must independently verify citizenship data through applicable State verification procedures and follow the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.
- Section VII of [Match 1051](#): The SSA Enumeration System database used for SSN matching is 100 percent accurate based on SSA's Office of Quality Review 'FY 2018 Enumeration Accuracy Review Report (April 2019).' This review includes the citizenship information provided at the time the individual applied for their SSNs. However, there is no obligation for an individual to report to SSA a change in his or her citizenship or immigration status until he or she requests a replacement card or files a claim for a Social Security benefit. While the citizenship information is accurate for SSA's program purposes, if used later for other purposes, it may not be current. SSA is not the custodian of U.S. citizenship records.

Page 3 – Jon Sherman

- Section X of [Match 1097](#): SSA's assessment of its citizenship data indicates that approximately ¼ of those records do not have an indication of citizenship present. However, SSA notes that while the indication of citizenship present in its records has increased over the years, it still only represents a snapshot in time. Accordingly, while SSA may have more records with an indication of citizenship, this information may not be available at the time of SSA's data exchange with CMS.

See Computer Matching Programs (ssa.gov) (providing a copy of all SSA matching agreements).

Testimony Denial

An agency employee may appear in a legal proceeding to which the agency is not a party and testify about any SSA function or any information or record SSA created or acquired as a result of the discharge of official duties. However, under SSA regulations, such appearance and testimony require the prior authorization of the Commissioner or her designee. 20 C.F.R. § 403.100. Similar regulations governing Federal employee testimony have consistently been upheld as legitimate. *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951); *Smith v. Cromer*, 159 F.3d 875 (4th Cir. 1998); *Swett v. Schenk*, 792 F.2d 1447 (9th Cir. 1986).

We may consider several factors in determining whether to authorize testimony in cases in which SSA is not a party. Those factors include but are not limited to: the risk of violation of law or compromise of Government privilege; the burden on SSA; and the interest served by allowing the testimony. 20 C.F.R. § 403.130. Your application does not establish the criteria necessary to allow an SSA employee to testify.

While your request may not risk violation of law, granting your request for testimony would burden the agency and unduly expend the resources of the agency for a lawsuit that does not involve SSA. See 20 C.F.R. § 403.130(b). To provide the requested testimony, SSA would be required to divert at least one SSA employee from his or her assigned duties, thereby reducing SSA's ability to timely perform its own work, with no counterbalancing benefit to SSA. See 20 C.F.R. § 403.130(b)(1). Moreover, as explained above, the information sought is available through public information. See 20 C.F.R. § 403.130(b)(2). In addition, this request presumes SSA would be authorized to share such information with the State of Arizona and we have not identified any request from the State of Arizona to share such information for this purpose, or agency approval to such data sharing.

Further, we have considered the interests that would be served by providing testimony in this case and find that the testimony would not serve SSA's interests. 20 C.F.R. § 403.130. While a state government official is involved in this case, permitting testimony would provide no benefit to SSA as SSA has no interest in the outcome of this case. 20 C.F.R. § 403.130(c)(2)-(3). Moreover, the testimony is not needed to prevent fraud or misconduct, prevent a miscarriage of justice, or preserve the rights of an accused individual to due process in a criminal proceeding. See 20 C.F.R. § 403.130(c)(4)-(5).

Page 4 – Jon Sherman

Thank you for your cooperation in this matter. If you have any questions, please contact Marty Budetti at (913) 219-0672.

Sincerely,

/s/ Jessica Vollmer for

Nancy Morales Gonzalez
Associate General Counsel
for General Law, Division 1

Exhibit 20



SOCIAL SECURITY

December 18, 2006

The Honorable Jim McCrery
Chairman, Subcommittee on Social Security
Committee on Ways and Means
House of Representatives
Washington, D.C. 20515

Dear Mr. McCrery:

I am pleased to provide you with the enclosed report addressing your April 7, 2006 letter, requesting an assessment of the accuracy of Social Security Administration's (SSA) Numident fields that are relied on by the Basic Pilot—a Department of Homeland Security (DHS) employment eligibility verification service.

Thank you for bringing your concerns to my attention. My office is committed to combating fraud, waste, and abuse in SSA's operations and programs. The report highlights various facts pertaining to the issues raised in your letter. To ensure SSA, DHS and the Department of State are aware of the information provided to your office, we are forwarding a copy of this report to the Inspectors General for each of these agencies.

If you have any questions concerning this matter, please call me or have your staff contact H. Douglas Cunningham, Assistant Inspector General for Congressional and Intra-Governmental Liaison, at (202) 358-6319.

Sincerely,

A handwritten signature in black ink, appearing to read "Patrick P. O'Carroll, Jr.", written in a cursive style.

Patrick P. O'Carroll, Jr.
Inspector General

Enclosure

cc:
Jo Anne B. Barnhart

CONGRESSIONAL RESPONSE REPORT

Accuracy of the Social Security Administration's Numident File

A-08-06-26100



December 2006

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- Promote economy, effectiveness, and efficiency within the agency.**
- Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- Independence to determine what reviews to perform.**
- Access to all information necessary for the reviews.**
- Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

Executive Summary

OBJECTIVE

To assess the accuracy of the Social Security Administration's (SSA) Numident fields that are relied on by the Basic Pilot.

BACKGROUND

As of November 2005, SSA had assigned about 435 million Social Security numbers (SSN)—for the primary purpose of accurately reporting and recording the earnings of people who work in jobs covered by Social Security. When SSA assigns an SSN to an individual, the Agency creates a master record in its “Numident” file containing relevant information about the numberholder.

SSA provides employers with a number of verification programs and services that allow them to match employees' names and SSNs with SSA's records. Additionally, the Basic Pilot, a Department of Homeland Security (DHS) program supported by SSA, provides employers a tool for determining whether newly-hired employees reported the correct name, SSN, date of birth and are authorized to work in the United States. Recently, the House and Senate each passed immigration reform bills that would mandate employers' use of an employment eligibility verification system similar to the Basic Pilot. Given the extent and significance of this proposed legislation, it is essential that the Numident file contain correct information.

On April 7, 2006, we received a request from the Honorable Jim McCrery of the House Committee on Ways and Means, Chairman of the Subcommittee on Social Security, to assist the Subcommittee in obtaining information on the reliability of SSA data used in the Basic Pilot program to verify employment eligibility. In particular, the Chairman asked that we assess the accuracy of SSA Numident fields that are relied on by the Basic Pilot. The Chairman specified that we determine Numident accuracy rates for each of the following populations: (1) native-born U.S. citizens, (2) foreign-born U.S. citizens, and (3) non-U.S. citizens. To address his request, we reviewed 810 randomly-selected Numident records in each of these populations (a total of 2,430 records) to determine their accuracy and whether data discrepancies might result in inaccurate feedback from the Basic Pilot. Because SSA does not delete, destroy, rescind, inactivate or cancel SSNs once they are assigned,¹ we selected our sample of all SSNs the Agency had assigned as of November 30, 2005.

RESULTS OF REVIEW

We cannot predict the types of documentation each of the tested numberholders might present to an employer when attempting to prove their identities and authorization to

¹ Programs Operations Manual System, RM 00201.040.

work in the United States—as the current process allows a number of varying sources of this information.² Accordingly, our audit conclusions only pertain to the accuracy of SSA’s Numident file when compared to (1) information SSN numberholders provided to SSA when applying for their original and/or replacement Social Security cards and, if applicable, (2) certain data elements DHS had for the Numident records tested. Despite these limitations, we found SSA’s Numident file information to be generally accurate.

We identified some discrepancies that could result in the Basic Pilot providing incorrect feedback to employers attempting to determine the employment eligibility of their workers. Specifically, of the 2,430 Numident records reviewed, 136 contained discrepancies in the name, date of birth or citizenship status of the numberholder or we determined that the numberholder may be deceased.³ In all of these cases, the Basic Pilot provided incorrect results. As a result, we estimate that discrepancies in approximately 17.8 million⁴ (4.1 percent) of the 435 million Numident records could result in incorrect feedback when submitted through the Basic Pilot. While the accuracy of SSA’s Numident records is noteworthy, if use of an employment verification service such as the Basic Pilot becomes mandatory, the workload of SSA and DHS may significantly increase—even if only a portion of these 17.8 million numberholders need to correct their records with one of these agencies.

We are particularly concerned with the extent of incorrect citizenship information in SSA’s Numident file for the foreign-born U.S. citizens⁵ and non-U.S. citizens we tested. Based on DHS information, we determined that 62 (7.7 percent) of the 810 foreign-born U.S. citizen Numident records we reviewed were misclassified—and the numberholders were not actually U.S. citizens. Given this exception rate, we estimate that about 616,420 of the approximate 8 million numberholders in the foreign-born U.S. citizen

² Presently, up to 29 documents issued by various Federal, State and local awarding agencies are valid for completing the *Employment Eligibility Verification* (Form I-9), which is legally required for every newly-hired employee. Acceptable records include (1) DHS identity and work authorization documents; (2) U.S. passports; (3) SSN cards; (4) State and local Government records; and (5) records from schools, medical facilities and the military. See 8 C.F.R. § 274a.2; DHS Form I-9.

³ Of the 136 discrepancies, 42 (30.9 percent) were on Numident record entries dated before May 15, 1978, the date on which SSA began requiring all SSN applicants to provide proof of age, identity and U.S. citizenship. The remaining 94 (69.1 percent) Numident records were dated between May 15, 1978 and November 30, 2005.

⁴ This estimate was developed using a stratified sampling approach. We randomly selected 810 Numident records from each of the three populations. The three populations varied in size based on the citizenship status and place of birth annotated on the Numident records. See Appendix C for our sample results.

⁵ Foreign-born U.S. citizens are those individuals who (1) were born abroad to U.S. citizen parents or (2) became “naturalized” citizens after immigrating to the United States. 8 U.S.C. §§ 1401(c); 1421 *et seq.*

category are not actually U.S. citizens.⁶ Additionally, we noted that 57 (7.0 percent) of the 810 non-U.S. citizen Numident records we reviewed were currently misclassified—because the individuals had become U.S. citizens after obtaining their SSN but had not updated their records with SSA. Although SSA is not at fault for these latter misclassifications, we estimate that of the 46.5 million non-U.S. citizen records in SSA's Numident file, about 3.3 million contain out-of-date citizenship status codes.⁷ As such, these individuals may need to visit an SSA office to correct their Numident record before they would be confirmed eligible for employment by the Basic Pilot.

CONCLUSION

Given the scope and breadth of information held in SSA's Numident file, we applaud the Agency on the accuracy of the data we tested. However, we estimate that approximately 17.8 million Numident records contain discrepancies that may result in incorrect Basic Pilot feedback to employers. As Congress considers legislation requiring mandatory verification of all U.S. workers' employment eligibility through a system such as the Basic Pilot, we believe it should examine the significant workload that may result from the millions of numberholders whose Numident records may need to be corrected. Our review showed that the Numident records for these individuals have discrepancies in the numberholders' names, dates of birth, citizenship status and/or death indications that would result in inaccurate feedback from the Basic Pilot.

Because our tests included SSNs that were assigned decades ago, we recognize that some numberholders would no longer be working and would not attempt to correct their SSA and/or immigration records. However, if even a portion of the estimated numberholders whose Numident records contained discrepancies were required to visit an SSA office to correct their information, the Agency's workload may significantly increase until such time as the affected records were corrected.

⁶ As explained on pages 10 and 11 of this report, only 19 of these cases were included in the total 136 discrepancies that impacted Basic Pilot results. Although the remaining 43 foreign-born U.S. citizens discussed were misclassified, DHS confirmed that they were Legal Permanent Residents and authorized to work. As such, the Basic Pilot feedback was correct – they were eligible for employment.

⁷ We believe this is a conservative estimate because DHS was only able to provide citizenship data for 506 of the 810 non-U.S. citizens in our sample.

Table of Contents

	Page
INTRODUCTION	1
RESULTS OF REVIEW	5
Native-Born U.S. Citizens.....	6
Foreign-Born U.S. Citizens.....	9
Non-U.S. Citizens.....	11
CONCLUSION	14
OTHER MATTER	15
APPENDICES	
APPENDIX A – Acronyms	
APPENDIX B – Scope and Methodology	
APPENDIX C – Sample Results	
APPENDIX D – Basic Pilot	
APPENDIX E – Additional Discrepancies that Did Not Impact Basic Pilot Results	

Introduction

OBJECTIVE

To assess the accuracy of the Social Security Administration's (SSA) Numident fields that are relied on by the Basic Pilot.

BACKGROUND

As of November 2005, SSA had assigned about 435 million Social Security numbers (SSN)—for the primary purpose of accurately reporting and recording the earnings of people who work in jobs covered by Social Security. When SSA assigns an SSN to an individual, the Agency creates a master record in its “Numident” file containing relevant information about the numberholder. This information includes the numberholder’s name, date of birth, place of birth, parents’ names, citizenship status, date of death (if applicable) and the office where the SSN application was processed and approved. Additionally, the Numident record for each numberholder identifies (1) any changes to the original information provided by the numberholder (for example, name changes, revisions to citizenship status) and (2) an account of all replacement SSN cards obtained.

The first explicit statutory authority to issue SSNs was enacted in 1972.¹ Before that time, SSNs were issued pursuant to administrative procedures that the Agency had established. At the inception of the program, all SSNs were assigned and cards issued based solely on information provided by the applicant. Evidence of identity was not required. However, beginning in November 1971, persons age 55 and over applying for an SSN for the first time were required to submit evidence of identity. As of April 1974, noncitizens were required to submit documentary evidence of age, identity and immigration status. In May 1978, SSA began requiring all SSN applicants to provide evidence of age, identity and U.S. citizenship or noncitizen status.² In addition, as of September 2002, SSA began verifying all immigration documents with DHS before assigning SSNs to noncitizens.

¹ Social Security Amendments of 1972, Pub. L. 92-603, 86 Stat. 1329 (1972).

² Subject Counterfeiting and Misuse of the Social Security Card and State and Local Identity Documents: Hearing Before the House Committee on the Judiciary, Subcommittee on Immigration and Claims, 106th Cong., 1st Sess. 64 (1999) (statement of Glenna Donnelly, Assistant Deputy Commissioner, Office of Disability and Income Security Programs, SSA).

SSA posts an employee's wages to its Master Earnings File (MEF)³ based on a *Wage and Tax Statement* (Form W-2) submitted by his or her employer.⁴ However, these earnings can only be posted successfully to a numberholder's MEF record if the name and SSN reported on the Form W-2 match the information on SSA's Numident file for that individual. For example, if the Numident record for a numberholder contains a last name that significantly differs from what the employer provided on the Form W-2, the earnings will not be posted to the individual's earnings record—and, if not corrected, will not be counted towards the numberholder's future Social Security benefits. Additionally, if an employee falsely uses a name and/or SSN to work in the United States, which does not match the associated Numident record, these wages will not be posted to the correct numberholder's account.

To prevent these name and SSN discrepancies, SSA provides employers and third parties⁵ with a number of verification programs and services that allow them to verify employees' names and SSNs against SSA's records before submitting the Form W-2s.⁶ To ensure correct responses to employers through these verification services, it is essential that SSA's Numident records are as accurate and complete as possible.

On April 7, 2006, we received a request from the Honorable Jim McCrery of the House Committee on Ways and Means, Chairman of the Subcommittee on Social Security, to assist the Subcommittee in obtaining information on the reliability of SSA data the Department of Homeland Security (DHS) uses to verify employment eligibility. In particular, the Chairman asked that we assess the accuracy of SSA Numident fields that are relied on by the Basic Pilot. The Chairman specified that we determine Numident accuracy rates for each of the following populations: (1) native-born U.S. citizens, (2) foreign-born U.S. citizens, and (3) non-U.S. citizens.

BASIC PILOT

The Basic Pilot is a DHS initiative supported by SSA through a Memorandum of Understanding between the two agencies. The purpose of the Basic Pilot is to assist employers in verifying the employment eligibility of newly-hired employees.

³ The MEF, formally known as the Earnings Recording and Self-Employment Income System, Social Security Administration, Office of Systems, SSA/OS 60-0059, contains all earnings data reported by employers and self-employed individuals. SSA uses the data to determine eligibility for and the amount of Social Security benefits. 71 Federal Register (FR) 1796, 1819-1820 (January 11, 2006).

⁴ The *Social Security Act* § 205(c)(2)(A), 42 U.S.C. § 405(c)(2)(A) requires SSA to maintain records of wage amounts employers pay to individuals.

⁵ A third party would be a company or individual that submits or requests information on behalf of someone else.

⁶ While our review focuses on the Basic Pilot, SSA offers other types of employee verification services. These tools include SSA's Employee Verification Service for Registered Users, which allows employers to submit employees' names/SSNs via paper or magnetic media, and the Social Security Number Verification Service, an on-line verification system. Unlike the Basic Pilot, these tools do not allow employers to verify the work authorization status of employees.

Participating employers register on-line with DHS to use the automated system. Information the employer submits to DHS is first sent to SSA to verify that the SSN, name, and date of birth match SSA data contained on the employee's Numident record. If SSA verifies this information and no date of death is recorded on the Numident record, SSA provides DHS with U.S. citizenship information for the individual—as annotated on the numberholder's most recent Numident record. If the employee alleges U.S. citizenship and the Numident record also indicates the individual is a U.S. citizen, the Basic Pilot then notifies the employer that work authorization is confirmed. If a discrepancy is noted, the Basic Pilot sends the employer an "SSA tentative nonconfirmation" response.

After SSA verifies the SSN, name and date of birth of noncitizens, the Basic Pilot confirms current authorization to work in the United States with DHS.⁷ If a discrepancy occurs with an employee's work authorization, the Basic Pilot sends the employer a "DHS tentative nonconfirmation" response. In the case of either an SSA or DHS tentative nonconfirmation, the employee is provided an opportunity to correct the information contained in SSA and/or DHS records. See Appendix D for more information on the Basic Pilot.

SCOPE AND METHODOLOGY

To achieve our objective, we reviewed a total of 2,430 SSNs that SSA assigned from 1936 through November 2005. We recognize that our tests included SSNs that were assigned decades ago and some of these numberholders would no longer be working and/or attempting to correct their SSA and/or immigration records. However, we included all SSNs the Agency had assigned up to November 30, 2005, in our universe because SSA does not delete, destroy, rescind, inactivate or cancel SSNs once they are assigned. Accordingly, older SSNs could still be used—appropriately or inappropriately—for employment purposes.

We selected our samples from a segment of SSA's Numident file as of November 30, 2005.⁸ Specifically, as shown in Table 1, we reviewed 810 Numident records for SSNs within each of the following 3 populations: (1) native-born U.S. citizens, (2) foreign-born U.S. citizens, and (3) non-U.S. citizens.

⁷ The determination as to whether a noncitizen is currently authorized to work rests with DHS—the Basic Pilot places no reliance on work authorization information SSA has in its records in making this determination.

⁸ SSA stores Numident records in equal segments by arranging records in numerical order according to the last two digits of the SSN (for example, 80-84, 85-89, 90-94, etc). Each segment represents 5 percent of all Numident records and there are 20 segments in total. It is common practice for SSA to use a segment to estimate results to the entire file.

Table 1: Details of Sample Selected for Review

Column A	Column B	Column C	Column D
Category	Sample Size	Number of SSNs in Segment 3 of Numident File (as of 11/30/05)	Estimate of Total SSNs In Numident File for Each Category (Column C x 20)
Native-Born U.S. Citizens	810	19,010,361	380,207,220
Foreign-Born U.S. Citizens	810	402,667	8,053,340
Non-U.S. Citizens	810	2,326,218	46,524,360
Total	2,430	21,739,246	434,784,920

Our tests compared the Numident data (name, SSN, date of birth and citizenship status) to copies of the original *Application for a Social Security Card* (Form SS-5) and, when applicable and available, copies of applications for replacement Social Security cards to ensure that SSA personnel accurately entered the information provided by the applicant. Additionally, we attempted to determine the legitimacy of any dates of death present on Numident records. Further, we attempted to verify noncitizens' and foreign-born U.S. citizens' "citizenship" status with DHS or the Department of State (State). We also submitted the 1,620 U.S. citizen SSNs through the Basic Pilot, using information provided by the numberholder on his or her Form SS-5. Finally, we submitted all noncitizen SSN records through the Basic Pilot when we could obtain DHS alien registration or admission numbers⁹ or when we identified any discrepancies between SSA and DHS information for the numberholder.

Underlying Assumptions

In performing our tests, we could not predict what proof of identity and work authorization a numberholder would present to an employer. Therefore, we made the following assumptions.

- The information provided by the numberholder on his or her Form SS-5(s) was correct and would be the same data provided to an employer.
- The information provided by DHS and/or State was correct.

See Appendix B for more information regarding our scope and methodology and Appendix C for our sample results.

⁹ The alien registration (or "A") number is the 9-digit number following "A" that is shown on the "green card" or *Permanent Resident Card* (Form I-551, formerly Form I-151 *Alien Registration Receipt Card*), the *Employment Authorization Document* (I-766 and I-688B), and on certain other immigration documents and notices. For newly admitted immigrants, the "A" number is shown on the machine-readable immigrant visa affixed to the foreign passport. The admission number is the 11-digit number located on the *Arrival-Departure Record* (Form I-94). Form I-94 shows the date the individual arrived in the United States, the "Admitted Until" date, and the date when his or her authorized period of stay expires. Form I-94 also usually shows the noncitizen's class of admission (for example, "F-1," which includes noncitizen academic students in colleges, universities, seminaries, conservatories, academic high schools, other academic institutions, or in language training).

Results of Review

SSA's Numident file represents an extensive repository of personal information provided by hundreds of millions of SSN applicants throughout the Agency's history. The primary purpose in maintaining this information is to ensure that U.S. workers receive appropriate credit for the wages they earned and, ultimately, to provide full and accurate benefits to entitled individuals. Recently, the House and Senate each passed immigration reform bills that would mandate employers' use of an employment eligibility verification system similar to the Basic Pilot.¹⁰ Given the extent and significance of the proposed legislation, it is essential that the Numident file contain correct information.

We cannot predict what documentation every numberholder tested might present to an employer when attempting to prove their identities and authorization to work in the United States—as the current process allows a number of varying sources of this information. Accordingly, our audit conclusions only pertain to the accuracy of SSA's Numident file when compared to (1) information SSN numberholders provided to SSA when applying for their original and/or replacement Social Security cards and, if applicable, (2) certain data elements DHS had for the Numident records tested. Despite these limitations, we found SSA's Numident file information to be generally accurate.

We identified some discrepancies that could result in incorrect feedback to employers attempting to verify employees' eligibility to work in the United States through the Basic Pilot. Specifically, of the 2,430 Numident records reviewed, 136 contained discrepancies that could result in inaccurate employment eligibility results—and, in most cases, additional work for SSA and DHS as employees attempt to correct their Numident and immigration records.¹¹ As a result, we estimate that data discrepancies in approximately 17.8 million (4.1 percent)¹² of the 435 million Numident records could result in incorrect feedback when submitted through the Basic Pilot.¹³ These discrepancies are outlined in Table 2.

¹⁰ S. 2611, 109th Cong., 2d Sess. § 301 (2006); H.R. 4437, 109th Cong., 2d Sess. Title VII (2006).

¹¹ Of the 136 discrepancies impacting Basic Pilot results, 7 resulted from differences between the Numident and applicants' Form SS-5s; 33 resulted from death indications on the Numident or other SSA records, which did not preclude confirmation of employment eligibility; and 96 resulted from differences in information contained on the Numident file and data provided to us by DHS (that is, numberholder's name, date of birth, or citizenship status.)

¹² This estimate was developed using a stratified sampling approach. We randomly selected 810 Numident records from each of the three populations. The three populations varied in size based on the citizenship status and place of birth annotated on the Numident records. See Appendix C for our sample results.

¹³ Additional minor discrepancies were identified between the names and dates of birth shown on the original Form SS-5s and the Numident records. However, Basic Pilot tolerances permitted employment eligibility confirmation of these records. Further information regarding these discrepancies is provided in Appendix E.

Table 2: Data Discrepancies in SSA's Numident File

Population	Data Fields				Total
	Name	Date of Birth	Death Indication	Citizenship Status	
Native-Born U.S. Citizens	2	2	23	0	27
Foreign-Born U.S. Citizens	4	2	0	19	25
Non-U.S. Citizens	14	3	10	57	84
Total	20	7	33	76	136

NATIVE-BORN U.S. CITIZENS

Generally, SSA Numident records for native-born U.S. citizens were accurate. Of the 810 Numident records reviewed in this population, we identified 27 (3.3 percent) discrepancies that may result in inaccurate employment eligibility feedback from the Basic Pilot. Given this accuracy rate, we estimate that of the approximately 380 million native-born U.S. citizen records in the Numident file, about 12.7 million contain discrepant information that may result in incorrect Basic Pilot feedback. As shown in Table 3, these discrepancies involved name, date of birth, and death information that did not match or had not been annotated on SSA's Numident file. Additionally, we noted that 19 (2.3 percent) of the 810 U.S. born citizen records we tested were age 90 and over, had no indication of death on any SSA record and were not currently receiving SSA benefits. While these individuals may still be alive and, in some rare cases working, the Basic Pilot has no edit that would require additional contact with these individuals before confirming employment eligibility. We encourage SSA and DHS to incorporate a step in the Basic Pilot requiring further verification of potential employees who have reached a pre-determined age and/or have some indication of death on an SSA system of record.

Table 3: Native-Born U.S. Citizen Record Discrepancies that May Affect Basic Pilot Results

<i>Data Field</i>	<i>Number of Discrepancies</i>
Name	2
Date of Birth	2
Death Indication	23
Total	27

Name and Date of Birth Discrepancies that Affected Basic Pilot Results

Two (0.24 percent) of the 810 native-born U.S. citizen Numident records tested contained inaccurate spellings of the numberholders' names—when compared to the associated Form SS-5s. When the proper names were tested in the Basic Pilot, it returned an “SSA tentative nonconfirmation” for each. Additionally, 2 (0.24 percent) other Numident records lacked a date of birth for the numberholders. When we tested the dates of birth provided on the numberholders’ Form SS-5s, the Basic Pilot returned an “SSA tentative nonconfirmation” response. As such, these individuals’ employment eligibility may not be initially verified through the Basic Pilot and the numberholders may need to correct their information with SSA.

Death Indication Discrepancies that May Affect Basic Pilot Results

SSA provides a death indicator in its responses to the Basic Pilot. However, we determined that 23 (2.8 percent) of the 810 native-born U.S. citizens within our sample may be deceased according to SSA records, yet the Basic Pilot confirmed employment eligibility for these numberholders. In seven of these cases, the Numident records had no indication that the numberholder was deceased, but other SSA records (that is, the Master Beneficiary Record or Supplemental Security Income Record¹⁴) provided a date of death for the individuals. In the other 16 cases, the Numident records were annotated with a transaction code of “D,” which indicates that a report of death was received by SSA, but the death was not confirmed.¹⁵

Although SSA may not have verified the deaths of these numberholders, we do not believe the Basic Pilot should confirm employment eligibility without some additional contact with these individuals. If someone presented themselves as one of these 23 individuals to an employer and provided the correct name, SSN and date of birth, the employer could incorrectly verify the individual’s employment eligibility through the Basic Pilot. Accordingly, we encourage SSA to reconcile the Numident with other SSA records and annotate Numident records when an indication of death is present. Additionally, we believe the Basic Pilot should issue a tentative nonconfirmation notice to employers that more investigation is necessary for individuals with a transaction code of “D” on the Numident record (and any other code SSA chooses to use for death indicators annotated from the aforementioned reconciliation). These suggestions are not intended to preclude verification entirely, but to require further inquiry and resolution before DHS confirms employment eligibility.

In response to a draft of this report, SSA requested that we note the following.

SSA is working with State governments to improve the current paper-based process which we believe will resolve some of the issues with the Numident record not being updated. However, the most efficient manner to improve timeliness and accuracy of State data is by using Electronic Death Reporting (EDR); a web-based automation of the death registration process. Our goal is to receive verified death data within 24 hours of receipt in the State repository and within 5 days of death. To achieve that goal we have currently awarded 31 State EDR development contracts. Fourteen States plus the District of Columbia and the jurisdiction of New York City have already implemented EDR. We expect that an additional 7 States in FY 2007 and 8 more States in FY 2008 should

¹⁴ SSA establishes a Master Beneficiary Record for each Old-Age, Survivors and Disability Insurance claimant and a Supplemental Security Income Record for every Supplemental Security Income applicant. These reports maintain pertinent information necessary to accurately pay benefits to the individuals. The information maintained includes identification data (name, SSN, date of birth, address), type and date of any disability, monthly benefit amounts, and the reason for terminating or suspending benefit payments. The SSA published Privacy Act notices for the Master Beneficiary Record, SSA/ORSIS, 60-0090, and for the Supplemental Security Income Record Display and Special Veteran’s Benefits, SSA/ODSSIS, 60-0103, in January 2006. 71 Federal Register (FR) 1796, 1826-1834 (January 11, 2006).

¹⁵ According to an SSA representative, the Agency last used the “D” transaction code in 1983.

implement EDR. Additionally, for the longer term, the provisions of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 give grants to the States to cross match birth and death records within and among the States, and give the lead for the funding of EDR to the Department of Health and Human Services (HHS). We continue to work with HHS for the transition of funding for EDR beginning this fiscal year.

Numberholders Age 90 and Over Receive No Further Screening by Basic Pilot

Of the 810 native-born U.S. citizens reviewed, we identified 19 (2.3 percent) individuals age 90 and over who had no indication of death on his or her Numident record or any other SSA system of record and were not currently receiving SSA benefits. The oldest of these numberholders would be 134 in 2006. While these are clearly old Numident records established before SSA implemented improved procedures for reporting and verifying deaths, we are concerned that the Basic Pilot has no control requiring additional investigation or contact with these numberholders before confirming employment eligibility. In fact, we tested these 19 individuals through the Basic Pilot and all were confirmed eligible for employment.

We acknowledge that an employer should raise their own concerns when an employee claims to have been born in 1872. However, to ensure that (1) no employee attempts to misuse the identity of a deceased or aged person and (2) the employer does not inadvertently or intentionally overlook the misuse of the aged person's name, SSN and date of birth, we believe the Basic Pilot should be revised to issue a notice to employers that more investigation is necessary when an employee is older than a pre-established age.¹⁶

¹⁶ In an October 2006 audit report *Effectiveness of the Young Children's Earnings Records Reinstatement Process* (A-03-05-25009), we made a similar recommendation regarding SSA's SSN verification service. Specifically, we recommended that, consistent with the Agency's disclosure policies, SSA modify the Employer Verification Service for Registered Users and SSN Verification Service to detect SSNs for children under age 7 to provide appropriate notice to employers and potentially reduce the number of future notices. SSA agreed with our recommendation.

Informal comments SSA provided in response to a draft of this report pointed out that it is illegal for employers to discriminate on the basis of age and that use of an indicator for individuals over a specified age would require a new or amended routine under the *Privacy Act of 1974* to permit disclosure. Further, the Agency stated that its Memorandum of Understanding with DHS would need to be modified to provide such an indicator. Finally, SSA pointed out that DHS Form I-9 already requires employers to certify that the documents submitted by an employee appear to be genuine and relate to that employee.

While we are sensitive to the possibility of age discrimination and understand the legal and contractual modifications that would be required, we continue to believe that the Basic Pilot should not routinely confirm employment eligibility for a 134-year old person—without, at the very minimum, some further conversation with that individual. The determination whether such a control should be implemented rests with SSA, DHS and Congress. However, we would be remiss if we did not point out this vulnerability in the current process.

FOREIGN-BORN U.S. CITIZENS

Of the 810 foreign-born U.S. citizen Numident records reviewed, 25 (3.1 percent) contained discrepant information that could result in incorrect employment eligibility feedback from the Basic Pilot. As a result, we estimate that about 248,560 of the approximately 8 million foreign-born U.S. citizen records contain discrepancies that may result in incorrect employment eligibility results from the Basic Pilot. As shown in Table 4, differences were noted between the name, date of birth or citizenship status SSA annotated on the 25 Numident records and data provided by (1) the numberholder on his or her Form SS-5 or (2) DHS. Further, we also noted that SSA documented an incorrect citizenship code for 43 (5.3 percent) other foreign-born U.S. citizens within our sample (which are not listed in Table 4.) However, these noncitizens were authorized to work in the United States, so the incorrect citizenship code did not impact the Basic Pilot results at the time of our review.

Table 4: Foreign-Born U.S. Citizen Record Discrepancies that May Affect Basic Pilot Results

<i>Data Field</i>	<i>Number of Discrepancies</i>
Name	4
Date of Birth	2
Citizenship Status	19
Total	25

Name and Date of Birth Discrepancies that Affected Basic Pilot Results

Of the 810 foreign-born U.S. citizen Numident records tested, we identified 4 (0.5 percent) discrepancies in the “name” field and 2 (0.2 percent) differences in the “date of birth” field that caused the Basic Pilot to issue “SSA tentative nonconfirmation” responses. In one case, when applying for an SSN, the numberholder documented on the Form SS-5 that her first name was “Sabrina.” However, SSA recorded the numberholder’s name as “Brina” in the Numident record. The Basic Pilot provides tolerances for some differences in the spelling of names. However, the Basic Pilot did not recognize these two names as the same individual. In five other cases, the name or date of birth SSA documented on the Numident record disagreed with information provided by DHS.¹⁷ These discrepancies also impacted Basic Pilot results and caused “SSA tentative nonconfirmation” responses.

Citizenship Status Discrepancies

Based on DHS information, we determined that 62 (7.7 percent) of the 810 foreign-born U.S. citizen records reviewed were not actually U.S. citizens. Because SSA does not maintain copies of documents SSN applicants present to the Agency, we were unable to determine whether these individuals presented false evidence of U.S. citizenship to SSA or Agency personnel simply miscoded the information.¹⁸ Despite the citizenship indications on SSA’s Numident records, these numberholders are not citizens and their work authorization status should be determined by DHS. We estimate that about 616,420 other numberholders in the foreign-born U.S. citizen population (which totals approximately 8 million) may have been improperly classified as U.S. citizens in SSA records.

Of the 62 misclassified numberholders, 43 are Legal Permanent Residents (LPR)¹⁹ and, as such, authorized to work in the United States. These 43 discrepancies did not result in incorrect Basic Pilot feedback because employers would have been accurately notified that these individuals were eligible for employment. However, if something changes with their LPR status (for example, emigration, deportation, or failure to renew their status), their permission to work in the United States may be taken away. In fact, one DHS study estimated that, between 1900 and 1990, one-quarter to one-third of all

¹⁷ In response to a draft of this report, SSA stated that in December 2005, the Agency began requiring noncitizens to show their legal name on the SSN card—as reflected on the immigration document. Before that date, noncitizens could use a name reflected on an identity document; however, the name on the immigration document should have been annotated on the Numident.

¹⁸ Only 4 of these 62 citizenship discrepancies occurred after September 2002, the month in which SSA began verifying all immigration documents with DHS.

¹⁹ LPRs are foreign nationals who have been granted the right to reside permanently in the United States. LPRs are often referred to simply as “immigrants,” but they are also known as “permanent resident aliens” and “green card holders.” LPRs are permitted to live and work anywhere in the United States, to own property, to attend public schools, to join certain branches of the Armed Forces, and they may also become U.S. citizens if they meet certain eligibility requirements.

LPRs emigrated from the United States.²⁰ Yet, the SSNs assigned to these individuals remain active. Therefore, the numberholders—or anyone posing as the numberholders—could continue to use the SSNs to work in the United States long after they are authorized to do so. Accordingly, we caution SSA and DHS that improper employment eligibility confirmations may eventually result from the incorrect citizenship status currently shown on these SSA records.

According to DHS, the remaining 19 misclassified numberholders needed further investigation before their work authorization status could be verified. Specifically, if SSA's citizenship codes had been correct for these numberholders, the Basic Pilot would have referred these records to DHS for review and possible contact with the numberholder before work authorization was established. Given the uncertainty of the numberholders' employment eligibility, we considered the discrepancies in SSA's citizenship codes to have caused improper Basic Pilot feedback and included these cases in Table 4.

NON-U.S. CITIZENS

Non-U.S. citizen (noncitizen) records within SSA's Numident file contained a much higher degree of error than the U.S. citizen populations. Specifically, of the 810 noncitizen records tested, 84 (10.4 percent) contained discrepancies that may result in inaccurate employment eligibility results from the Basic Pilot. As shown in Table 5, these discrepancies resulted from differences in names, dates of birth, citizenship status and death indications. Many of these differences were caused because the numberholder did not update his or her information with SSA (for example, the noncitizen did not notify SSA when he or she became a U.S. citizen). As a result, we estimate that of the approximately 46.5 million noncitizen records contained in SSA's Numident file, 4.8 million contain discrepancies that could require the numberholder to visit an SSA office to correct his or her Numident record before employment eligibility would be confirmed.

Additionally, as in the native-born U.S. citizen population, we identified 50 numberholders who were age 90 or over and had no indication of death present on their SSA records and were not currently receiving SSA benefits. As currently structured, the Basic Pilot would confirm employment eligibility for these individuals without any further contact or investigation.

²⁰ DHS, Office of Immigration Statistics Policy Directorate, publication *Estimates of the Legal Permanent Resident Population and Population Eligible to Naturalize in 2004*, issued February 2006.

Table 5: Non-U.S. Citizen Record Discrepancies that May Affect Basic Pilot Results

<i>Data Field</i>	<i>Number of Discrepancies</i>
Name	14
Date of Birth	3
Citizenship Status	57
Death Indication	10
Total	84

Name and Date of Birth Discrepancies that Affected Basic Pilot Results

Fourteen (1.7 percent) of the 810 Numident records tested contained numberholders' names that differed from either the individuals' Form SS-5 or DHS-provided data.²¹ When the alternate spellings were tested in the Basic Pilot, it returned an "SSA tentative nonconfirmation" for each. Additionally, 3 (0.4 percent) other Numident records contained a date of birth that differed from the Form SS-5 or DHS data. As such, these individuals' employment eligibility may not be initially verified through the Basic Pilot and the numberholders may have to correct their information with SSA.

Citizenship Status Discrepancies that Affected Basic Pilot Results

Based on DHS information, we determined that 57 (7.0 percent) of the 810 noncitizens tested were actually U.S. citizens—but had not updated their immigration/citizenship status with SSA. As a result, if these individuals alleged citizenship to an employer, the Basic Pilot would not initially confirm employment eligibility. Although SSA is not at fault for these misclassifications, we estimate that of the 46.5 million non-U.S. citizen records in SSA's Numident file, about 3.3 million contain incorrect citizenship status codes.²² As such, these individuals may need to visit an SSA office to correct their Numident records before they would be confirmed eligible for employment by the Basic Pilot.

²¹ In response to a draft of this report, SSA stated that in December 2005, the Agency began requiring noncitizens to show their legal name on the SSN card—as reflected on the immigration document. Before that date, noncitizens could use a name reflected on an identity document; however, the name on the immigration document should have been annotated on the Numident.

²² We believe this is a conservative estimate because DHS was only able to provide citizenship data for 506 of the 810 non-U.S. citizens in our sample.

Death Indication Discrepancies that May Affect Basic Pilot Results

Additionally, we determined that 10 (1.2 percent) of the 810 noncitizens within our sample may be deceased according to SSA records. However, the Basic Pilot confirmed employment eligibility for these numberholders. In seven of these cases, the Numident records had no indication the numberholder was deceased. Yet, other SSA records (that is, the Master Beneficiary Record) provided a date of death for the individuals. In the other three cases, the Numident records were annotated with a transaction code of “D,” which indicates that a report of death was received by SSA, but the death was not confirmed.

As previously mentioned in this report, we do not believe the Basic Pilot should confirm employment eligibility without some additional contact with these individuals. Rather, we believe SSA should first reconcile its records and annotate any indications of death on the Numident—if an indicator is not already present. Secondly, we believe the Basic Pilot should issue a tentative nonconfirmation notice to employers that more investigation is necessary for individuals with a transaction code of “D” on the Numident record (and any other code SSA chooses to use for death indicators annotated from the aforementioned reconciliation).

Numberholders Age 90 and Over Receive No Further Screening by Basic Pilot

Within the sample of 810 noncitizens reviewed, we identified 50 (6.2 percent) individuals age 90 and over who had no indication of death on his or her Numident record or any other SSA system of record and were not currently receiving SSA benefits. The oldest of these numberholders would be 139 in 2006. As mentioned previously in this report, we are concerned that the Basic Pilot has no control requiring additional investigation or contact with these numberholders before confirming employment eligibility. In fact, we tested these 50 individuals through the Basic Pilot and all were confirmed eligible for employment. As such, we believe the Basic Pilot should be revised to issue a notice to employers that more investigation is necessary when an employee is older than a pre-established age.

Conclusion

Given the scope and breadth of information held in SSA's Numident file, we applaud the Agency on the accuracy of the data we tested. However, we estimate that about 17.8 million Numident records contain discrepancies that may result in incorrect Basic Pilot feedback to employers. As Congress considers legislation requiring mandatory verification of all U.S. workers' employment eligibility through a system such as the Basic Pilot, we believe it should also consider the significant workload that may result from the millions of numberholders whose Numident records may need to be corrected. Our review showed that the Numident records for these individuals have discrepancies in the numberholders' names, dates of birth, citizenship status and/or death indications that would result in inaccurate feedback from the Basic Pilot.

Because our tests included SSNs that were assigned decades ago, we recognize that some numberholders would no longer be working and would not attempt to correct their SSA and/or immigration records. However, if even a portion of the estimated numberholders whose Numident records contained discrepancies were required to visit an SSA office to correct their information, the Agency's workload may significantly increase until such time as the affected records were corrected.

Other Matter

DHS' U.S. CITIZENSHIP AND IMMIGRATION SERVICES UNABLE TO LOCATE IMMIGRATION RECORDS FOR NONCITIZEN RECORDS

DHS' U.S. Citizenship and Immigration Services (USCIS) was unable to locate immigration records for 304 (37.5 percent) of the 810 noncitizen numberholders in our sample—through its computer data match. As such, for these numberholders, we could not determine whether SSA's Numident data matched DHS information (such as, name, date of birth and citizenship status). USCIS stated it could not match/locate these records through computer searches because of data compatibility problems. Specifically, USCIS' Central Index System records are organized by alien number (A-Number). Visitors or other noncitizens can be admitted under an I-94 Admission number. The records of these admissions are tracked in various DHS databases, primarily the Treasury Enforcement Communications System/Interagency Border Inspection System. We could only provide DHS with data SSA recorded on the noncitizen's Form SS-5 or in the Numident—which generally included the numberholder's name, date of birth, place of birth, parents' names, approximate date of entry to the United States (date of the SSN application) and, if SSA recorded it, the noncitizen's alien (A-number) or admission number.

We first requested immigration information from DHS for noncitizens in our sample on May 8, 2006. USCIS retained the services of a contractor, which used computer searches based on the numberholder's name and date of birth, in attempting to locate the records in USCIS' Central Index System. On occasion, USCIS also attempted to manually search its records for the individuals. On December 6, 2006, USCIS provided the following statement regarding its inability to match/locate some of these records.

Thank you for the opportunity to comment on those records USCIS was unable to match. The attached file you provided contains the names and information of data either not found or not matched in entirety in the Central Index System (CIS) or in manual records located here. SSA provided names and dates of birth in order for USCIS to match data and locate an A-number within USCIS' Central Index System to determine the Class of Admission. Past attempts to match SSA and USCIS data have shown that it is difficult to match records without a common numerical identifier between the two systems (Numident and CIS). Since SSA uses SSN and CIS is A-number driven it can be difficult to match records based solely on name and date of birth because slightly different names may be used with each agency, and names may change. Moreover, birth dates may be incorrect or miskeyed in one system or the other. Additionally, there may be more than one person with the same name and date of birth, making it impossible to know which record is the correct match.

It should be noted that the lack of a match does not mean the CIS system is deficient. It may well be the case that non-citizens who are not known to USCIS because they are illegal entrants have obtained SSNs, and thus have a

Numident record. Without knowing the specifics of each of the 304 cases, we cannot draw conclusions about whether the mismatch was due to inadequate information provided, or due to the fact that no USCIS record exists on the subject of the Numident record. The possibility that some are not known to USCIS because they are not lawful entrants should not be excluded.¹ USCIS Records Division has checked CIS to the best extent possible based on the names and information provided.

¹ **Footnote to USCIS Statement.** We would also note that a significant percentage of the records worked with overall in this study were older ones, which are the ones most likely to lack a corresponding USCIS record because they related to SSN's issued pre-1974, when SSA did not require proof of identity or citizenship, and thus are more likely to pertain to an unlawful alien than newer Numident records.

We believe certain aspects of USCIS' statement need further clarification. First, we provided USCIS more data than just the numberholders' names and dates of birth. Additionally, with respect to the footnote included in USCIS' statement, we would point out that 605 (74.7 percent) of the 810 noncitizen SSNs reviewed were assigned after April 15, 1974, the date on which SSA began requiring proof of alien status for noncitizens as part of the SSN application process. In fact, 347 (42.8 percent) were assigned after January 1, 1990. Further, of the 304 records USCIS could not match/locate, 184 (60.5 percent) of the SSNs were assigned after April 15, 1974. In fact, 127 (41.8 percent) of the 304 records were assigned after January 1, 1990.

We acknowledge that most noncitizen numberholders seeking employment would be able to provide employers their alien or admission number so that DHS could confirm their employment eligibility through the Basic Pilot. In many cases the newly hired employee shows his or her USCIS-issued documentation as proof of identity and work authorization, and this documentation includes an A-number or an I-94 Admission number. Noncitizens are required to carry their immigration documentation with them at all times, so these numbers should be readily available. USCIS advised us that in their operation of the Basic Pilot program and the evaluations they have been conducting for the last 7 years, they have not encountered lack of A-numbers or admission numbers on Form I-9 as a major concern raised by employers or employees participating in the Basic Pilot program. One of these DHS-issued numbers must be listed on the Form I-9 by all noncitizen new hires, whether or not their employer is participating in the Basic Pilot. Nevertheless, we are somewhat concerned with USCIS' inability to locate these records. If only a small portion of the 46.5 million noncitizen numberholders have forgotten or misplaced their alien or admission numbers, the workload for DHS may increase as these individuals attempt to confirm their employment eligibility and/or correct their immigration records.

Appendices

Appendix A

Acronyms

DHS	Department of Homeland Security
EDR	Electronic Death Reporting
HHS	Department of Health and Human Services
IRTPA	<i>Intelligence Reform and Terrorism Prevention Act of 2004</i>
MEF	Master Earnings File
OIG	Office of the Inspector General
SSA	Social Security Administration
SSN	Social Security Number
State	Department of State
U.S.	United States
U.S.C.	United States Code

Forms

I-9	<i>Employment Eligibility Verification</i>
I-94	<i>Arrival-Departure Record</i>
I-151	<i>Alien Registration Receipt Card</i>
I-551	<i>Permanent Resident Card</i>
I-766 and I-688B	<i>Employment Authorization Document</i>
SS-5	<i>Application for a Social Security Card</i>
W-2	<i>Wage and Tax Statement</i>

Appendix B

Scope and Methodology

To accomplish our objective, we performed the following steps.

- Reviewed pertinent sections of the Social Security Administration’s (SSA) policies and procedures as well as other relevant Federal laws and regulations.
- Reviewed Office of the Inspector General, Government Accountability Office and Department of Homeland Security (DHS) reports and other relevant documents.
- Randomly selected a segment of SSA’s Numident file as of November 30, 2005.¹ From the segment, we stratified the Social Security numbers (SSN) into three populations and randomly selected 810 Numident records for review from each: (1) native-born U.S. citizens, (2) foreign-born U.S. citizens and (3) non-U.S. citizens. Table 1 provides the actual number of SSNs in Segment 3, categorized by the aforementioned populations.

Table 1: Details of Sample Selected for Review

Column A	Column B	Column C	Column D
Category	Sample Size	Number of SSNs in Segment 3 of Numident File	Estimate of Total SSNs In Numident File for Each Category (Column C x 20)
Native-Born U.S. Citizens	810	19,010,361	380,207,220
Foreign-Born U.S. Citizens	810	402,667	8,053,340
Non-U.S. Citizens	810	2,326,218	46,524,360
Total	2,430	21,739,246	434,784,920

- For each sample item, we obtained copies of the original *Application for a Social Security Card* (Form SS-5) and any subsequent SS-5s that resulted in an update to the numberholder’s Numident record (for example, a name change or change in citizenship status.)
- We then compared the Numident data (name, SSN, date of birth, and citizenship status) to the SS-5s to ensure SSA personnel correctly recorded the information provided by the applicant.

¹ SSA stores Numident records in equal segments by arranging records in numerical order according to the last two digits of the SSN (for example, 80-84, 85-89, 90-94, etc). Each segment represents 5 percent of all Numident records and there are 20 segments in total. It is common practice for SSA to use a segment to estimate results to the entire file.

- We attempted to determine the legitimacy of any dates of death present on the Numident records, if applicable, by (1) researching SSA and other records to determine what State and/or jurisdiction the death occurred and (2) if located, requesting a copy of the death certificate from that location.
- For numberholders age 90 and over, who did not have a date of death annotated on their Numident records, we reviewed SSA's Master Beneficiary Record and Supplemental Security Income Record Display to determine whether a death indication was noted on these records for the individual and whether they were currently receiving SSA benefits.
- We verified foreign-born noncitizens' and foreign-born U.S. citizens' "citizenship" status with DHS and/or the Department of State (State).
- We obtained birth and, if applicable, marriage and/or death certificates for the first 50 sample items in each of the 3 populations.
- We submitted the 1,620 U.S. citizen SSNs through the Basic Pilot, using information provided by the numberholder on his or her Form SS-5. Further, we submitted all noncitizen SSN records through the Basic Pilot when we could obtain DHS alien or admission numbers or when we identified any discrepancies between SSA and DHS information for the numberholder.
- We summarized and projected our results to the entire Numident universe (all 20 segments) as of November 30, 2005. See Appendix C for our sample results.

Underlying Assumptions

In performing our tests, we could not predict what proof of identity and employment eligibility a numberholder would present to an employer. Therefore, we made the following assumptions.

- The information provided by the numberholder on his or her Form SS-5 was correct and would be the same data provided to an employer.
- The information provided by DHS and/or State was correct.

Our review of internal controls was limited to obtaining an understanding of SSA's SSN assignment process, the Numident file and the SSA/DHS Basic Pilot—and conducting the tests outlined above. The objective of our review was to determine the reliability of the Numident file. Accordingly, we determined that the Numident file information was generally reliable. However, we did not test the information provided by DHS and State. Accordingly, we cannot opine to its reliability. Any conclusions discussed in this report, which were predicated on information provided by DHS or State, have been annotated with the appropriate qualification.

The SSA entities audited were the Offices of Operations, Systems, and Income and Security Programs. We conducted the audit between April and November 2006 in Birmingham, Alabama. We conducted our audit in accordance with generally accepted government auditing standards.

Appendix C**Sample Results****Table 1: Sample Results and Projections for All Citizenship Categories**

U.S. Citizens (Native- and Foreign-born) and Non-U.S. Citizens	
Population of SSNs assigned since 1936 from one segment of the Numident file ¹	21,739,246
Sample Size	2,430
Attribute Projections	
Number of discrepancies in sample	136
Estimate of discrepancies in segment	887,344
Projection—Lower Limit	647,130
Projection—Upper Limit	1,127,558
Numident Estimate	
Estimate of discrepancies for the entire Numident file (887,344 x 20 segments)	17,746,880
<i>Projections made at the 95-percent confidence level.</i>	

¹ We estimate SSA assigned approximately 435 million SSNs between 1936 and November 2005 (21,739,246 in Numident segment 3 X 20 segments = 434,784,920).

Table 2: Sample Results and Projections For Individual Citizenship Strata

Native-Born U.S. Citizens	
Population of SSNs assigned 1936-November 2005 from one segment of the Numident	19,010,361
Sample size	810
Attribute Projection	
Number of discrepancies in sample	27
Estimate of discrepancies in segment	633,679
Numident Estimate	
Estimate of discrepancies for entire Numident file (633,679 x 20 segments)	12,673,580
Foreign-Born U.S. Citizens	
Population of SSNs assigned 1936-November 2005 from one segment of the Numident	402,667
Sample size	810
Attribute Projection	
Number of discrepancies in sample	25
Estimate of discrepancies in segment	12,428
Numident Estimate	
Estimate of discrepancies for entire Numident file (12,428 x 20 segments)	248,560
Non-U.S. Citizens	
Population of SSNs assigned 1936-November 2005 from one segment of the Numident	2,326,218
Sample size	810
Attribute Projection	
Number of discrepancies in sample	84
Estimate of discrepancies in segment	241,237
Numident Estimate	
Estimate of discrepancies for entire Numident file (241,237 x 20 segments)	4,824,740

Table 3: Other Projections for Foreign-Born U.S. Citizens

Foreign-Born U.S. Citizens—Misclassified in the Numident File	
Population of SSNs assigned 1936-November 2005 from one segment of the Numident	402,667
Sample size	810
Attribute Projection	
Number of individuals who were not citizens in sample	62
Estimate of number of individuals who are not citizens in segment	30,821
Numident Estimate	
Estimate of number of individuals who are not citizens in entire Numident file (30,821 x 20 segments)	616,420

Table 4: Other Projections for Non-U.S. Citizens

Non-U.S. Citizens—Misclassified in the Numident File	
Population of SSNs assigned 1936-November 2005 from one segment of the Numident	2,326,218
Sample size	810
Attribute Projection	
Number of instances in sample where citizenship was misclassified in sample	57
Estimate of discrepancies in segment	163,697
Numident Estimate	
Estimate of number of instances where citizenship was misclassified in entire Numident file (163,697 x 20 segments)	3,273,940

Appendix D

Basic Pilot

The Basic Pilot is a Department of Homeland Security (DHS) initiative, supported by the Social Security Administration (SSA) through a Memorandum of Understanding between the two agencies.¹ The purpose of the Basic Pilot is to assist employers in verifying the employment eligibility of newly-hired employees. The President signed *The Basic Pilot Program Extension and Expansion Act of 2003* (Public Law Number 108-156) into law on December 3, 2003. This law extended the operation of the Basic Pilot for an additional 5 years (to a total of 11 years) and expanded the operation to all 50 States not later than December 1, 2004.

As discussed with SSA and DHS staff, the Basic Pilot involves using the information in Government databases (SSA databases and, if needed, DHS databases) to determine the employment eligibility of new hires. The Social Security number (SSN) and Alien Registration Number ("A" Number) or I-94 Number (Admission Number) are used for these checks. The employer must complete the DHS-issued *Employment Eligibility Verification Form* (Form I-9) for each employee and then enter elements of this data into the Basic Pilot within 3 days of hiring, including the employee's SSN, name, date of birth, and whether the new hire indicated he or she was a U.S. citizen and, if not, the "A" Number or I-94 Number.

The system first checks the information entered against SSA's database to verify the name, SSN, and date of birth of newly-hired employees, regardless of citizenship. When the Numident indicates United States citizenship for the newly-hired employee and the new-hire indicated that he/she is a U.S. citizen, the Basic Pilot automated system confirms employment eligibility. If the Basic Pilot system cannot confirm employment eligibility based on the information in SSA's database or an "A" Number or I-94 Number was entered, the Basic Pilot system checks the data against DHS' database.

The employer will receive notification of "SSA tentative nonconfirmation" of employment eligibility when the SSN, name, or date of birth does not match the information in SSA's database or if a death indicator is present. Also, employers will receive an "SSA tentative nonconfirmation" if the new hire indicated he or she was a U.S. citizen and SSA's records did not show that the person was a U.S. citizen. The employer will receive notification of "DHS tentative nonconfirmation" of employment eligibility when DHS' database does not show the newly-hired noncitizen as authorized for employment. In these cases, the employer asks the employee whether he or she wishes to contest the tentative nonconfirmation. If contested, the employee must contact SSA or DHS within 8 Government working days of the notification. After the employee contacts SSA or DHS to correct the record, the employer resubmits the query through the Basic Pilot system. If the system does not confirm employment eligibility after the employer resubmits the query, the employer may terminate the new hire.

¹ Section 401 et seq. of the *Illegal Immigration Reform and Immigrant Responsibility Act of 1996* (8 U.S.C. §1324a), Pub. Law No. 104-208.

Appendix E**Additional Discrepancies that Did Not Impact
Basic Pilot Results**

Discrepancies that Did Not Impact Basic Pilot	Native-born U.S. Citizens	Foreign-born U.S. Citizens	Non-U.S. Citizens
Name	13	167	160
Date of Birth	9	9	16
Citizenship	0	43	43
Totals:	22	219	219

DISTRIBUTION SCHEDULE

Commissioner of Social Security
Office of Management and Budget, Income Maintenance Branch
Chairman and Ranking Member, Committee on Ways and Means
Chief of Staff, Committee on Ways and Means
Chairman and Ranking Minority Member, Subcommittee on Social Security
Majority and Minority Staff Director, Subcommittee on Social Security
Chairman and Ranking Minority Member, Subcommittee on Human Resources
Chairman and Ranking Minority Member, Committee on Budget, House of Representatives
Chairman and Ranking Minority Member, Committee on Government Reform and Oversight
Chairman and Ranking Minority Member, Committee on Governmental Affairs
Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives
Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives
Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate
Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate
Chairman and Ranking Minority Member, Committee on Finance
Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy
Chairman and Ranking Minority Member, Senate Special Committee on Aging
Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.

Exhibit 21



U.S. Department of Justice

Civil Rights Division

Office of the Assistant Attorney General

Washington, D.C. 20530

August 14, 2025

Via Mail and Email

The Honorable Chuck Gray
Secretary of State
Herschler Building East
122 West 25th Street, Suite 100
Cheyenne, WY 82002-0020

(b)(6)

secofstate@wyo.gov

Re: Complete Wyoming's Voter Registration List with All Fields

Secretary Gray:

We have received Wyoming's statewide voter registration list ("VRL"). However, as the Attorney General requested, the electronic copy of the statewide VRL must contain *all fields*, including the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")¹ to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We have requested Wyoming's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501, *et seq.* Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).

The Help America Vote Act ("HAVA"), 52 U.S.C. § 20501, *et seq.*, also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA's computerized statewide Voter Registration List requirements. *See* 52 U.S.C. § 21111; *see also Brunner v. Ohio Republican Party*, 555 U.S. 5, 6

¹ In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that Justice Department be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

(2008) (*per curiam*) (finding there is no private right of action to enforce those requirements in HAVA).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of 22 months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is demanding an electronic copy of Wyoming’s complete and current VRL. The purpose of the request is to ascertain Wyoming’s compliance with the list maintenance requirements of the NVRA and HAVA.

When providing the electronic copy of the statewide VRL, Wyoming must ensure that it contains *all fields*, which includes the registrant’s full name, date of birth, residential address, his or her state driver’s license number or the last four digits of the registrant’s social security number as required under the Help America Vote Act (“HAVA”)² to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

Moreover, HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 552a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained in the Driver’s License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency’s function to accomplish its enforcement authority as the Justice Department is now doing.

² In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that Justice Department be able to conduct an independent review of each state’s list. Any statewide prohibitions are clearly preempted by federal law.

That said, all data received from you will be kept securely and treated consistently with the Privacy Act.

In charging the Attorney General with enforcement of the voter registration list requirements in HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are preempted by federal law.

To that end, please provide the requested electronic Voter Registration List³ to the Justice Department within seven days or by August 21, 2025.

The information and materials may be sent by encrypted email to voting.section@usdoj.gov or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). Should further clarification be required, please contact Maureen Riordan at (b)(6)

Regards,



Harmeet K. Dhillon
Assistant Attorney General
Civil Rights Division

cc: Charles Young, Director, Elections Division
Herschler Building East
122 West 25th Street, Suite 99
Cheyenne, WY 82002-0019
Elections@wyo.gov

³ Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.

Exhibit B

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF ELENA NUNEZ ON BEHALF OF COMMON CAUSE

I, Elena Nunez, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am a U.S. citizen, over the age of 18, am competent to testify, and have personal knowledge of the facts and information set forth in this declaration.

2. I am a member of Common Cause. As a full-time member of Common Cause's staff, I currently serve as Senior Vice President, States. I have served in this role and a substantially similar role since 2018 and have been a member of Common Cause's staff since 2007.

3. In my role as Senior Vice President, States, I directly oversee all Common Cause state operations and support Common Cause work across the country, including our work to protect voting rights, promote ethical government, and hold power accountable. I also engage with Common Cause's policy, organizing, and external affairs staff to advance pro-voter, pro-democracy policy. I supervise my team's work with multiple coalitions to advance pro-voter reforms and increase civic engagement, including the national Election Protection Coalition.

4. Common Cause is a nonprofit, nonpartisan membership organization incorporated under the laws of the District of Columbia. Pursuant to its bylaws, Common Cause is organized

and operated as a membership organization and acts in this action on behalf of itself and in a representative capacity on behalf of its members.

5. Pursuant to its bylaws, Common Cause has defined who qualifies as a member. Under its definition, a “member” of Common Cause is any individual who, within the past two years, (a) made a financial contribution to the organization; or (b) has taken meaningful action in support of Common Cause’s advocacy work. Such meaningful action includes, but is not limited to, signing petitions directed to government officials; participating in letter-writing or phone-banking campaigns; attending town halls, workshops, or rallies organized by Common Cause; or otherwise engaging in activities designed to advance the organization’s mission. As of this writing, there are nearly one million members of Common Cause nationwide.

6. Common Cause Education Fund (CCEF), an affiliated charitable nonprofit, provides education, engagement, and research to Common Cause members, constituents, partner organizations, and the public about voter registration and the electoral process. CCEF works to create public engagement on democracy issues and promote effective citizen participation, which is critical for a healthy and robust democratic society. For purposes of this declaration, references to “Common Cause” include the activities and operations of both Common Cause and CCEF.

7. Common Cause has staff in 21 states (Arizona, California, Colorado, Florida, Georgia, Hawaii, Indiana, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, Texas, and Wisconsin). Although we lack on-the-ground staff in some states, Common Cause has members in every state in the country, including other states that have shared their voter rolls with the federal government, such as Alaska, Arkansas, Kansas, Louisiana, Mississippi, Oklahoma, South Carolina, South Dakota, Tennessee, and Wyoming. Through our work with the Election

Protection Coalition, we support partners' work on election protection in states where we do not have staff. I also engage with Common Cause's policy, organizing, and external affairs staff to advance policies designed to protect the rights of all eligible Americans to vote, including in states where we do not physically have staff.

8. Common Cause's mission is to uphold the core values of American democracy by creating an open, honest, and accountable government that serves the public interest, promotes equal rights, opportunity, and representation for all, and empowers people to make their voices heard in the political process.

9. Common Cause believes the right to vote is the cornerstone of a functioning democracy. We are committed to ensuring that every eligible voter can register and cast their ballot, with a focus on communities who experience additional barriers to participation including Black people, Indigenous Peoples, Latina/o people, Asian/Pacific Islanders, other people of color, naturalized citizens, justice impacted individuals, young people, seniors, and people with disabilities. Through our legislative advocacy, Common Cause has ensured that voting around the country has remained as accessible as possible for eligible voters. Part of that work is to counter unlawful government conduct that could chill or prevent participation in the election process, such as unreliable ways of verifying voter eligibility and purging of voter registrations.

10. As part of its core mission, Common Cause works on a nonpartisan basis to expand and protect equal access to voting for all citizens on multiple fronts, including: (a) lobbying for nonpartisan election reforms, including, but not limited to, allowing no-excuse absentee voting, extending the deadlines for submitting mail-in ballots, increasing the number of voting locations, and ensuring a fair, nonpartisan redistricting process; (b) providing education and training to on-the-ground voting rights activists throughout the country; (c) working with

other community organizations to track problems at voting sites on Election Day, field calls from voters who experience burdens in their efforts to exercise their fundamental right to vote, and provide assistance to such voters by lobbying local election officials and/or facilitating their access to counsel; and (d) advocating for nonpartisan election reforms, such as an expansion of early voting, designed to promote racial equity by removing barriers to the franchise disproportionately borne by communities of color.

11. Common Cause assists voters across the country in registering to vote, verifying, and/or updating their voter registration through outreach to our members in each state. For example, on National Voter Registration Day, Common Cause members and supporters across the country receive notices from us urging them to register to vote and/or to verify their registration status via tools embedded on our website. In 2024, nearly 6,000 voters registered to vote using the Common Cause web tools, and nearly 40,000 more verified their registration using these tools. Common Cause also engages in policy advocacy around voter registration and list maintenance issues and either directly registers voters or assists coalition partners who conduct voter registration.

12. Common Cause also works to ensure that once registered, all voters can cast a ballot during early voting, on Election Day, or through absentee or mail-in voting. As Election Protection is one of our core organizational programs, Common Cause co-leads the national Election Protection Coalition to help Americans across the country navigate the voting process and cast their ballot without obstruction, confusion, or intimidation. Election Protection is the largest body of work for our state staff, particularly during an election year. Common Cause advances this work in a number of ways, including by managing and facilitating poll observation programs, which train volunteers to be present at polling locations to help identify issues and

obstacles to voting that prospective voters may experience. Volunteers are trained to help voters when they are unable to vote, such as when the voter is present at the wrong polling location. Our Election Protection program not only works to directly assist voters with access to the ballot, it helps us identify systemic problems so we can develop strategies to address them in the future.

13. Common Cause has been committed to ensuring that registered voters are not erroneously removed from the voter list, because deleting a voter registration creates a risk of disenfranchisement. In various states that have attempted to adopt flawed data-matching processes designed to purge voter registrations, Common Cause has responded by engaging in advocacy to oppose such practices, bringing litigation to challenge those policies, and, where such processes are being implementing, conducting public education campaigns to remind voters to verify their registration status in advance of an election. In particular, Common Cause has opposed the use of the so-called SAVE system to determine voter eligibility, because the SAVE system contains systemic flaws that cause it to misidentify voters as non-citizens. We know from the federal government's own admission that citizenship data from the Social Security Administration and the Department of Homeland Security is filled with errors. Removing voter registrations based on flawed or error-prone processes directly undermines Common Cause's mission of ensuring that every eligible voter can register and cast their ballot.

14. In Common Cause's experience, data-related errors are especially likely to occur for those who have naturalized or derived citizenship, those who have had name changes or variations in the spelling of their name, those born prior to 1981, those who have recently moved, and those with former felony convictions whose rights have been restored. Common Cause does not collect such data for all of our members, but we know through outreach efforts and other communications that our membership includes many individuals in these categories.

For example, in South Carolina, which Common Cause understands recently entered into an agreement to provide voter data to the Department of Justice (“DOJ”), Common Cause was able to identify several dozen members who fall into at least one of the above categories in only two days’ time.

15. If DOJ is allowed to use state voter data to direct the purging of voters’ registrations using the SAVE system, that will directly impair Common Cause’s organizational mission of promoting democracy and enabling and empowering citizens to engage in the political process. It will force us to redirect our resources from our core programming and activities, in the same way that past attempts to use the SAVE system and conduct voter purges have forced Common Cause to expend resources in order to protect the right to vote. For example, we have previously had to dedicate staff time to conduct direct outreach to members in Texas to help identify voters who may have been wrongly flagged for removal from the voter rolls based on faulty data from the SAVE system. In North Carolina, the State Board of Elections’ plans to use the SAVE system have required our staff to work with partners to analyze the impact of the proposed rules, submit public comment with proposed revisions, and educate members about the rulemaking and how to submit public comment.

16. If DOJ is allowed to continue collecting state voter data—and subsequently disclose it to the Department of Homeland Security or other entities, including contractors—that will also directly impair Common Cause’s organizational mission of promoting political participation. Because of questions and concerns about the privacy of voter data and the possible misuses of such data, particularly due to the sharing of voter data with an agency responsible for immigration enforcement, Common Cause will have to devote staff time and other resources to create educational materials, update trainings, and expend greater resources in order to assist and

engage voters. For example, Common Cause anticipates that citizens living with undocumented family members will be among those who are more hesitant to register to vote as a result of DOJ sharing voter data with Department of Homeland Security. DOJ's actions therefore make Common Cause's work to register and engage voters more difficult and less effective.

17. Common Cause members will also be harmed by DOJ's collection and disclosure of voter data. Common Cause has more than 140,000 members residing in Alaska, Arkansas, Indiana, Kansas, Louisiana, Mississippi, Nebraska, Ohio, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, and Wyoming alone (states that may have provided voter data to DOJ). DOJ's failure to adhere to legal requirements protecting private data while collecting and disclosing data puts many of these members' personal information at risk. Our members have a privacy interest in their own data, and Common Cause, as the organization that assisted many of them in registering or updating their registration, has an interest in protecting the integrity and privacy of that data. Any threat to the security of voter data, especially one that could result in the misuse of personal information, directly undermines our work, damages public trust, and risks chilling voter participation.

18. To advance our mission, Common Cause also engages in the policymaking process by submitting comments in response to federal notices of rulemaking and policies. For example, when the Department of Homeland Security published a System of Records Notice in 2025 detailing its plans to repurpose the SAVE database for voting purposes, Common Cause and over 24,000 Common Cause members submitted comments opposing the change. Over 30,000 members joined Common Cause in submitting comments on a similar notice from the Social Security Administration. In the past five years, Common Cause has commented on rulemaking notices from various federal agencies including DOJ, the Election Assistance

Commission, the Federal Trade Commission, the National Telecommunications and Information Administration, the Census Bureau, and more.

19. Had DOJ provided notice and opportunity for the public to offer comments on its policy to gather and maintain state voter data, conduct list maintenance on it, and share it with the Department of Homeland Security and other third parties, Common Cause would have participated in that process. Common Cause would have submitted its views, among others, that the DOJ lacks the legal authority to gather and maintain state voter data, that voters have concerns about potential misuse of their data, that the sharing of voter data with the Department of Homeland Security and other entities is likely to deter voter registration and participation, that collecting and sharing such data places Common Cause's members and other voters' information at risk, and that the federal SAVE system is not a reliable process for determining voter eligibility.

20. Common Cause has limited resources. When new obstacles to voting appear, we need to increase our education and advocacy efforts to respond. We are already creating materials and responding to questions from our coalition partners and members who are concerned about the potential impact of DOJ's policy. For example, in Nebraska, our state staff faced a massive increase in questions from the public following the DOJ's request for the state's voter rolls. We expect that we will need to adapt our election protection trainings and voter education materials to address voter questions and confusion.

21. If voters are purged from voter rolls, as contemplated in the agreements that DOJ has made with some states, we will need to increase our voter outreach and education to make sure voters know how to respond. We have had to respond to voter needs like this in the past. For example, after Florida eliminated the permanent vote by mail list, our Florida staff and partners

needed to do voter education and outreach to voters (phonebanks) to inform them of the changes in the law and what voters needed to do to continue to vote by mail. After a purge of nearly 95,000 voters from the voter rolls in Texas, our Texas staff did outreach to alert voters of the changes and provide information on registration. This additional assistance is essential to our current and core mission and function of helping people register and vote. When anyone, in this case the federal government, throws more obstacles in the way of eligible voters, we need to educate and assist voters in addressing those obstacles. As a result, our state staff are already planning to dedicate even more time to Election Protection than they may have in an ordinary election year, causing them to have less time for other organizational priorities. Anything less would depart from and diminish a central and longstanding mission of the organization.

22. Common Cause is planning Election Protection programs for various primary and general elections occurring between now and November. Uncertainty about the DOJ's actions is interfering with our ability to prepare and execute our election plans. An important part of our work is to be a trusted resource for coalition partners, voters, and the public about voting laws, policies, and practices. The information the DOJ refuses to disclose is necessary for us to provide accurate information. If we provide information that is incorrect or incomplete, there is a risk of voters being disenfranchised. Not providing accurate guidance would also damage our hard-earned reputation and goodwill.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and that this Declaration was signed in New York City, NY, on May 15, 2026.

A handwritten signature in black ink, appearing to read 'E NUNEZ', written over a horizontal line.

ELENA NUNEZ

Exhibit C

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF GAVIN GEIS ON BEHALF OF COMMON CAUSE

I, GAVIN GEIS, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am a U.S. citizen, over the age of 18, am competent to testify, and have personal knowledge of the facts and information set forth in this declaration.

2. I have been a member of Common Cause since 04/01/2012. I currently serve as the State Director for Common Cause in Nebraska. I have served in this role since 07/01/2013.

3. In my role, I am responsible for all Common Cause operations in Nebraska, including our work to protect voting rights, promote ethical government, and hold power accountable. I work with multiple coalitions to advance pro-voter reforms and increase civic engagement, including through in-person testimony on relevant state legislation, public education via Common Cause and partner events, engagement with members of the press, advocacy with legislators, and through organizing Nebraskans to make their voices heard in the political process.

4. As of this writing, there are nearly one million members of Common Cause nationwide, approximately 4,300 of whom are in Nebraska.

5. There are two Common Cause staff members responsible for carrying out the organization's mission in Nebraska. The staff in Nebraska consists of myself and a state organizer.

6. Consistent with Common Cause's mission nationally, Common Cause's mission in Nebraska is to create open, honest, and accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all people to make their voices heard in the political process.

7. In Nebraska, Common Cause works on a nonpartisan basis to expand and protect equal access to voting for all citizens on multiple fronts, including by: (1) educating voters about new laws and policies, including by developing informational materials and serving as an expert on election administration and election law changes for partner organizations involved in voter registration; (2) coordinating election protection efforts, including by coordinating a poll monitoring program with partner organizations; (3) advocating for greater access to voting, such as enacting a constitutional provision regarding a right to vote and opposing the use of the federal SAVE system for voting purposes; (4) protecting democratic processes, including the public ballot measure process in the state.

8. The collection of voter data from Nebraska by the U.S. Department of Justice ("DOJ") has already burdened Common Cause's work in the state and made executing its mission more difficult.

9. In order to carry out Common Cause's mission effectively and address the concerns of voters and partner organizations, I have to keep myself and the other staff updated on new legal and political developments pertaining to voting and elections. I have found it very difficult to keep up to date with all of the latest developments, including locating information

about Nebraska's voter data and who it may have been disclosed to. Since Fall 2025, we have spent roughly 20 hours contacting state and local election officials in an effort to understand what data they are sharing with DOJ and what agreements they have with the federal government regarding the data-sharing. That included contacting the Nebraska Secretary of State to see if he intended to share the state voter database with DOJ. We did not receive clear answers from the state and pursued litigation to block the state from releasing voter data; the case is still pending before the Nebraska Supreme Court. The issue of voter information and data privacy is at the nexus of voting rights and government access and transparency and has been an important issue for Common Cause, particularly in Nebraska, for years.

10. Since DOJ began gathering voter data, Nebraskans' interest in data privacy and security has exploded; I estimate that there has been a tenfold increase in the questions we've received on this subject. The inquiries have come from people expressing fear of their voter data getting leaked or wrongfully disclosed, particularly sensitive information like social security numbers; and individuals who are fearful of political retaliation and voter purges, particularly naturalized citizens who feel vulnerable. For example, I've spoken with one individual who fears being targeted by voter roll purges due to their naturalized status and is concerned about potential disruption to any family member's immigration proceedings.

11. If DOJ's efforts to gather and misuse voter data is not stopped, we will need to create public education materials explaining DOJ's actions and its impact on voters. I anticipate that our materials will focus on naturalized citizens, as well as married voters who have name changes, because, in our experience, those individuals are among the most likely to be misidentified as non-U.S. citizens due to gaps in government databases. Purging voter registrations based on unreliable information and deterring people from participating in our

democracy undermines Common Cause's mission and makes our efforts to engage voters less effective.

12. Similarly, if DOJ's efforts to remove registered voters from the rolls is not blocked, we will need to revise the trainings and training materials that we provide to our poll monitors. Together with our coalition partners, we train approximately 200 volunteers in an election year, to cover about 300 polling locations in the state. Our monitors are trained to answer questions from voters and to identify and report any issues they observe, such as inaccessibility and improper signage. Unless DOJ's actions are stopped, we will need to update our training materials, such as voter FAQs, to address the privacy concerns that many voters have. We will also have to train our volunteers to identify and assist voters who may be turned away because their voter registration has been purged. Because of the risk that eligible voters may be prevented from voting, we will have to prioritize our poll monitoring program and devote more resources towards recruiting and training volunteers in order to protect voters from being disenfranchised by DOJ's actions. This would require us to divert attention from our work engaging with Nebraskans in rural communities on the creation of voting districts and the impact of money on our elections. Additionally, we would need to engage in a public education campaign to remind voters to check their registration status to ensure they have not been purged from the rolls. This would require the diversion of our existing resources, redirecting at least 100 hours of worktime away from our current programs, with the possibility of greater diversion depending on the extent of voter roll purges and needs of voters.

13. In order to create educational or training materials, it is important that we have access to complete and accurate information about the processes and procedures related to voting and elections in the state. Unless we obtain full and accurate information from DOJ about its

intended uses of voter data, the security of DOJ's data practices, the persons that have access to Nebraskan voters' data, and the process for removing Nebraskan voters' registrations, we face a significant risk of misinforming voters and the broader public. Providing incorrect information to voters, volunteers, partner organizations, or the public in general could lead to disenfranchisement and would likely damage Common Cause's good will and reputation, which the organization has worked hard to build up and maintain for years.

14. Typically, we begin our voter education and volunteer efforts in Nebraska 4 months before an election. This year, because elections are taking place on May 12th and November 3rd, we began our election-related efforts on February 1st and will continue our efforts through November. If we did not begin by that date, we would lose the time and opportunity to engage voters before the election. Had DOJ disclosed information about its collection and use of voter data earlier, we could have already trained our volunteers and educated voters on those issues before the May election.

15. Common Cause's other programs and priorities in Nebraska include campaign finance reform, fair redistricting reform, public education on state sunshine laws, government accountability work, and partnership with underrepresented communities to identify barriers to participation in the democratic process.

16. Common Cause has limited resources to effectuate its mission, including in Nebraska. Because our state organizer and I have limited capacity, we have to pick and choose which programs and initiatives to prioritize. The DOJ's inserting itself into the voter registration and election administration processes in Nebraska has created new obstacles to political participation and already caused us to devote more resources to explaining data privacy and security concerns. Due to DOJ's ongoing actions, we have been forced to delay our public

education work on political spending in Nebraska by eight months and have not had the capacity to engage like we have previously with Nebraskans on legislation introduced during the 2026 Nebraska legislative session. Unless the DOJ's actions are blocked, it will further force us to divert resources from other priorities critical to Common Cause's mission.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and that this Declaration was signed in Lincoln, NE on May 14, 2026.

Gavin Geis

GAVIN GEIS

Exhibit D

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF JULIA VAUGHN ON BEHALF OF COMMON CAUSE

I, JULIA VAUGHN, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am a U.S. citizen, over the age of 18, am competent to testify, and have personal knowledge of the facts and information set forth in this declaration.

2. I currently serve as State Director of Common Cause in Indiana. I have served in a substantially similar role since 2022 and have been a member of Common Cause's staff since 1994.

3. In my role, I am responsible for all Common Cause operations in Indiana, including our work to protect voting rights, promote ethical government, and hold power accountable. To fulfill these responsibilities I lead the All IN for Democracy coalition, develop strategies and messaging for the coalition and Common Cause in Indiana, educate and organize our members, lobby the Indiana General Assembly, serve as the organization's spokesperson, recruit and develop advisory board members and work with volunteers, conduct fundraising activities, and supervise staff.

4. As of this writing, there are nearly one million members of Common Cause nationwide, approximately 17,600 of whom are in Indiana.

5. There are two Common Cause staff members primarily responsible for carrying out the organization's mission in Indiana, consisting of myself and an organizer. We also occasionally have a part-time intern.

6. Consistent with Common Cause's mission nationally, Common Cause's mission in Indiana is to reduce barriers to voting and give all voters an equal voice in elections. We also work to reduce the influence of big money on the political and legislative process, and to make campaign finance and lobbying expenditures more transparent. We work to register voters, particularly those in marginalized communities, and to educate them about why elections matter and help them gain the information they need to be informed voters.

7. In Indiana, Common Cause works on a nonpartisan basis to expand and protect equal access to voting for all citizens on multiple fronts, such as: (1) coordinating Election Protection efforts, including by coordinating a poll monitoring program with partner organizations; (2) educating voters about voting-related laws and policies; (3) registering new voters, particularly in under-served communities; (4) advocating for greater access to voting, such as by opposing the use of the federal SAVE system and other flawed databases to determine eligibility to vote; and (5) promoting democracy and representation, such as by opposing the drawing of gerrymandered districts and encouraging local communities to pass ordinances creating bipartisan citizens redistricting commissions.

8. Common Cause's other programs and priorities in Indiana include advancing open government and transparency measures and advocating against any law enforcement agency actions that deny any person of due process and their other constitutional rights.

9. The Department of Justice ("DOJ") gathering of voter data has already burdened Common Cause's work in Indiana and made executing its work more difficult.

10. In order to successfully register voters, Common Cause staff must keep up to date on changes to voting-related policies and procedures, such as requirements that voters provide documentary proof of citizenship and processes for purging voter registrations.

11. Voter registration is a regular part of Common Cause's work in Indiana, with staff (and trained volunteers) conducting voter registration events approximately 2–3 times a month in an election year such as this year. Common Cause staff in Indiana has focused on voter registration in under-served communities, including in low-income neighborhoods and with groups representing naturalized citizens and households with mixed immigration statuses. Common Cause staff also prioritizes voter registration programs with individuals who may have been involved with the criminal justice system in the past and are regaining their right to vote.

12. Based on Common Cause's experience working with these communities, we are concerned that voters will be reluctant to register when their information will be shared with federal law enforcement agencies, such as DOJ or the Department of Homeland Security. Immigration enforcement has been an issue of especially heightened concern in communities that Common Cause serves. Those concerns have spread across Indiana, where people are on high alert for possible immigration enforcement. For example, Common Cause staff recently observed approximately 200 people attend a protest against Immigration and Customs Enforcement in Carmel, a relatively high-income suburb.

13. Common Cause staff has also seen voters express concern and anxiety that their registration may be removed or made inactive. In the months since the DOJ announced they were collecting voter data from states, when we talk about these issues with voters we frequently hear that, even though they are regular voters, they check their voter registration at indianavoters.in.gov before every election because they fear being wrongfully purged from the

voting roll. Leading up to the May 2026 primary election at least 10 individuals expressed concern about themselves or people they knew being removed from the roll. In all of these cases, I communicated with the individuals and informed them of how to check their registration on state websites.

14. In Common Cause's experience, a lack of trust in the government makes convincing people to register to vote and participate in politics much more difficult. For example, because of the extreme amounts of money in elections, people we speak with tend to believe that elected officials only listen to wealthy special interests and well-connected people instead of advancing the interests of ordinary people.

15. Because of concerns about privacy and DOJ gathering of sensitive voter data, Common Cause staff in Indiana has already had to spend time and resources to respond. The Common Cause Indiana Executive Director leads the All IN for Democracy coalition, which meets regularly. After the Indiana Secretary of State turned over the voter file last summer, several coalition meetings have focused on the topic of protecting voters from unauthorized uses of this data on the agenda. We and our partners have spent time trying to understand how this information was transmitted and what parameters, if any, were put in place to protect voters. We have also spent time discussing how to respond to this situation and how to educate our members about the risks to their personal information. Common Cause staff in Indiana is a source of expertise on changes in voting-related laws and policies, and actions like DOJ collecting voter data, which has not been a transparent process, make it more difficult for Common Cause staff to keep partners and voters informed about potential new barriers to voting.

16. In order to accurately inform partners and voters, it is important that Common Cause has access to complete and accurate information about the processes and procedures

related to voting and elections. Unless we obtain full and accurate information from DOJ about its intended uses of voter data, the security of the agency's data practices, the persons that have access to Indiana voters' data, and the process for removing Indiana voters' registrations, we face a significant risk of misinforming voters and the broader public. Providing incorrect information to voters, volunteers, partner organizations, or the public in general could lead to disenfranchisement and would likely damage Common Cause's good will and reputation, which the organization has worked hard to build up and maintain for years.

17. Election Protection is a major area of work for Common Cause staff in Indiana that has been ongoing since 2008. Those efforts include training volunteers to answer voter questions and distribute palm cards containing information about the election and hotlines for seeking further assistance. Volunteers will also be stationed at polling locations to identify and report voting-related issues to Common Cause staff using a checklist. Due to lack of sufficient volunteers, Common Cause staff must prioritize 50–60 locations in Marion and Hamilton counties where issues are likely to occur. Common Cause staff has to train volunteers on new legal developments, such as when the State began requiring documentary proof of citizenship.

18. Common Cause anticipates having to train Election Protection volunteers to look for and assist voters who may be prevented from voting as a result of their voter registration being removed or rendered inactive as a result of DOJ using the SAVE database. Volunteers are typically trained to spot issues such as long lines, illegal electioneering, or people being at the wrong polling place. Common Cause's volunteers are limited in number and have limited capacity—requiring them to assist an additional category of potentially disenfranchised voters makes them less effective at addressing other issues that arise at polling locations and also make Common Cause's training efforts more complicated and time-consuming.

19. Typically, we begin our voter education and volunteer efforts in Indiana months before an election. For example, we began preparing for the May primary in March, and we will begin outreach for the general election in September. If we do not have the information we need to educate the public by then, we would lose the time and opportunity to engage voters before the election.

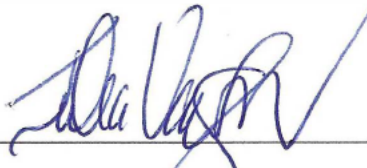
20. In response to past efforts by the State of Indiana to purge voters, Common Cause has sued to stop such efforts and worked to remind voters to check their voter registration status before an election. Common Cause anticipates needing to engage in similar public education efforts if DOJ attempts to use the SAVE system to remove or deactivate voter registrations in Indiana. Common Cause has had to engage in similar efforts in response to Indiana purging voters based on inaccurate lists obtained from the state DMV. When new processes are implemented that impact voter registration, Common Cause volunteers typically receive more questions and generate more calls to me as well as to the voter assistance hotline.

21. Because Common Cause only has a two-person staff in Indiana, Common Cause must pick and choose which priorities to focus on. When an urgent and unforeseen issue arises that threatens voters' ability to participate in the democratic process and receive fair representation, Common Cause has to put other programs and activities on hold in order to respond to the emergency. For example, in response to an unexpected mid-decade effort to redraw Indiana's congressional districts in a way that went against our organization's commitment to fair representation, Common Cause effectively put all other work on hold in order to advocate against the attempted redistricting for almost 5 months.

22. Purging of qualified voters and deterring political participation undermine Common Cause's mission and make our work of engaging voters less effective. If DOJ's

attempts to collect and nationalize voter registration is not stopped, Common Cause staff in Indiana will likely be forced to focus its attention on mitigating the risk of erroneous purging of voter registrations, including by conducting public education campaigns to remind voters to confirm their registration status and by recruiting and training volunteers to identify and assist impacted voters. As a result, Common Cause staff in Indiana will likely be forced to divert resources and staff time from other priorities in the State, such as advocacy on lobbying reform and legislative ethics, passing local redistricting reform, conducting a civic education campaign on the Far-Eastside of Indianapolis and starting a civic leadership training program for young Black voters in Indianapolis.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and that this Declaration was signed in Indianapolis, Indiana on May 15, 2026.



JULIA VAUGHN

Exhibit E

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

**DECLARATION OF CATHERINE TURCER ON BEHALF OF COMMON
CAUSE**

I, CATHERINE TURCER, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am a U.S. citizen, over the age of 18, am competent to testify, and have personal knowledge of the facts and information set forth in this declaration.

2. I have been a member of Common Cause for over a decade. I currently serve as State Director in Ohio. I have served in this or a substantially similar role since 2012.

3. In my role, I am responsible for all Common Cause operations in Ohio, including our work to protect voting rights, and promote ethical, transparent, and accountable government. I coordinate and supervise the other Common Cause Ohio-based employees.

4. As of this writing, there are nearly one million members of Common Cause nationwide, approximately 34,000 of whom are in Ohio.

5. There are three Common Cause staff members responsible for carrying out the organization's mission in Ohio, consisting of myself, a voting and elections manager, and an associate director. We are also planning to bring on an Election Protection organizer to join our staff this summer in advance of the election.

6. Consistent with Common Cause’s mission nationally, Common Cause’s mission in Ohio is to uphold the core values of American democracy. Our work focuses on state and federal government: We work to create open, honest, and accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all people to make their voices heard in the political process.

7. In Ohio, Common Cause works on a nonpartisan basis to expand and protect equal access to voting for all citizens on multiple fronts, including by: (1) coordinating election protection efforts as part of the Ohio Voter Rights Coalition, including recruiting and training volunteers for a poll monitor program and promoting the 866-OUR-VOTE hotline; (2) serving as an expert on changes in laws and policies affecting voting and elections in Ohio; (3) observing and monitoring proceedings conducted by the boards of elections; (4) protecting democratic processes, including by opposing legislation and directives from the Ohio Secretary of State that would undermine access to the ballot and the right to vote in Ohio, and (5) developing and deploying voter education resources to partners, volunteer educators, and voters.

8. Common Cause’s other programs and priorities in Ohio include promoting fair courts, open government, and equitable redistricting, as well as exposing corruption and pushing for government accountability. Our work includes pushing back against government overreach and promoting due process and civil rights.

9. The Department of Justice’s (“DOJ’s”) gathering of voter data has already burdened Common Cause’s work in Ohio and made executing its work more difficult.

10. Common Cause staff in Ohio are experts on election administration. Other organizations turn to Common Cause for regular briefings and updates, including on DOJ’s collection of voter data and the resulting privacy issues. Common Cause staff frequently join

calls with partner organizations to share information on election rules and processes; provide quarterly briefings to coalition partners; host monthly meetings with Common Cause members from Ohio; hold bi-weekly coalition member calls with updates; and provide media alerts and public comments on changes to the Secretary of State's election official manual, as an example.

11. Ohio's Secretary of State collaborated with DOJ by turning over voter rolls in February 2026. The Secretary of State and DOJ provided no information about why this data transfer was necessary, the purpose of the transfer or the process at the time of action. Ohio's sharing of voter data with the federal government has caused the Ohio staff at Common Cause to spend significant time working to understand federal use and investigation of Ohio's voter records. This includes seeking to understand a recent Department of Homeland Security visit to a Dayton Career Center related to a voter registration drive, and the federal government's public records requests for specific voter information, including voting history, from multiple county boards of elections. Common Cause's job of educating the public and other groups is made very difficult by the total lack of transparency surrounding both the use of the federal SAVE system and the process for investigating and removing voters from the rolls. Common Cause has worked hard to build its reputation as an expert when it comes to elections and election procedure, and the lack of available information related to the federal government's collection and use of voter data threatens to undermine our mission. Common Cause staff in Ohio intends to update our briefing materials by August 2026 at the latest to reflect DOJ's use of voter data.

12. Common Cause has also been engaging in nonpartisan Election Protection work in Ohio since 2012, as a leading organization in the Ohio Voting Rights Coalition and its steering committee. The Election Protection program includes recruiting and training volunteers to monitor outside of polling locations, during both early vote and on Election Day; reporting out

from county boards of elections meetings; running a peacekeeper program at the polls; promoting the Election Protection hotline; planning for attacks on elections and election results; and creating social media and other advocacy toolkits. Volunteer poll monitors undergo an hour-long training process, receive a checklist to spot potential issues at the polls, and learn how to speak with and assist voters. Poll monitors are also trained to identify people who may have been required to cast a provisional ballot instead of a regular ballot, based on a voter exiting a polling location with a provisional ballot informational handout. Having more voters purged or denied the ability to cast a regular ballot will result in poll monitors having to assist more people, which would detract from their ability to make sure that polling locations are not presenting other issues, such as long lines, inadequate access or signage, reports of equipment issues, electioneering, or voter intimidation. In Ohio, it is very difficult to cure provisional ballots, and Common Cause staff and volunteers do not have capacity to help large numbers of voters who are required to vote provisionally.

13. Due to the lack of official information from DOJ regarding its plans for maintaining and using voter data from Ohio, Common Cause staff has had to spend significant time attempting to investigate and find out what federal, state, and local officials have planned to do. The secrecy and lack of transparency are extremely disruptive. For example, a few months ago, when a reporter uncovered actions related to voter registration taken by the Secretary of State that were not publicly disclosed at the time, Common Cause had to stop what we were doing and divert resources to researching the issue, answering requests from the media and partners, updating our volunteer educators, and responding to related activity. Common Cause and voting rights coalition partners have met with election officials to better understand and compare how SAVE changes will be implemented across different counties, created press

statements to alert the public and the media, developed and updated training materials for Election Protection volunteers and voter education advocates. We've also identified the need to create a new legal volunteer role for Ohio's Election Protection efforts to help us prepare to help protect voters and continue our work adjacent to related federal action. Since December 2025, Common Cause has spent more than 75 hours working to investigate, build relationships, and respond to reports around understanding the current unknowns of federal involvement in Ohio's voter registration. Since very little information comes out of the Ohio Secretary of States' office directly, our team spends significant time searching through local media reports to further research related action or actors, building a timeline of events and potential impacts to voters.

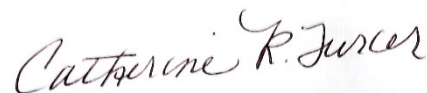
14. These efforts have diverted staff time and resources away from voter education. There is already a significant amount of voter confusion around federal and state voting laws in response to proposed federal legislation, executive orders, and comments from the executive branch on social media: the public does not necessarily differentiate between unsubstantiated commentary and enacted law, so Common Cause steps in to try to clarify. Common Cause routinely needs to answer questions from voters about what identification and credentials they need to vote. We also work in close coalition with voting rights organizations to educate voters on a larger scale by developing materials, FAQ sheets, social media tool kits and informational presentations. However, our ability to convey accurate information is already at a deficit when we cannot point to primary government sources to fact check information, especially when countering unsourced and unverified posts on social media. The lack of government transparency prevents us from doing one of the more crucial parts of our work – holding the government accountable to the people. A recent scandal resulted in the former Speaker of the Ohio House

going to federal prison; it is clear that policies need to be established to ensure that we can root out corruption and ensure transparency and accountability.

15. Common Cause staff also promotes political participation by encouraging people to register to vote and to check their voter registration status. Common Cause staff also help register voters and answer questions about voter registration at community events when there is an opportunity to do so.

16. DOJ's seizure of voter data and the government's lack of transparency make it more difficult for Common Cause staff to reassure people who are concerned about their information being collected and shared. In Common Cause's experience engaging voters, it already is difficult to persuade people to opt in and engage politically, but it is much harder to persuade people who do not trust the government. Purging voter registrations based on unreliable information and deterring people from participating in our democracy undermines Common Cause's mission and makes our efforts to engage voters less effective.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and that this Declaration was signed in Arlington, MA on May 15, 2026.



CATHERINE TURCER

Exhibit F

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

**DECLARATION OF ANTHONY GUTIERREZ ON BEHALF OF COMMON
CAUSE**

I, ANTHONY GUTIERREZ, pursuant to 28 U.S.C. § 1746, hereby declare as follows:

1. I am a U.S. citizen, over the age of 18, am competent to testify, and have personal knowledge of the facts and information set forth in this declaration.

2. I am a member of Common Cause, and I currently serve as State Director in Texas. I have served in a substantially similar role and have been a member of Common Cause's staff since 2016.

3. In my role, I am responsible for all Common Cause operations in Texas, including our work to protect voting rights, promote ethical government, and hold power accountable. I also manage three employees, as well as temporary Democracy Fellows, act as our chief spokesperson, and am responsible for fundraising and overseeing our budget.

4. As of this writing, there are nearly one million members of Common Cause nationwide, approximately 40,000 of whom are in Texas.

5. There are four Common Cause staff members who are primarily responsible for carrying out the organization's mission in Texas. The staff in Texas consists of myself, a policy

director, a program manager, and a digital organizer. Separate from the permanent staff, Common Cause also hosts several Democracy Fellows each semester. We currently have seven Democracy Fellows.

6. Consistent with Common Cause’s mission nationally, Common Cause’s mission in Texas is to advance and protect democracy in the State. Our work focuses on state and federal government: We work to create open, honest, and accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all people to make their voices heard in the political process.

7. In Texas, Common Cause works on a nonpartisan basis to expand and protect equal access to voting for all citizens on multiple fronts, including by: (1) educating voters about new laws and policies; (2) coordinating election protection efforts, including by recruiting and training poll observers; (3) advocating for reforms in election administration at the county and local levels; and (4) protecting democratic processes, by advocating for campaign finance and redistricting reforms.

8. Common Cause’s other priorities in Texas include serving as a watchdog for issues related to government ethics and corruption, advocating for campaign finance reforms, and leading the Texas Election Reform Coalition—a coalition of nonpartisan national and state organizations who work on voting rights.

9. The Department of Justice (“DOJ”) gathering of voter data has already burdened Common Cause’s work in Texas and made executing its work more difficult.

10. Increasing voter participation is one of the core objectives for Common Cause in Texas, which has one of the lowest participation rates in the country. To achieve that goal, Common Cause staff in Texas engages in public education campaigns to raise awareness of

election deadlines and election-related changes. Common Cause staff creates a range of materials, including public-facing materials for voters as well as toolkits for organizational partners who are part of the Texas Election Reform Coalition. Common Cause spends resources on advertisements and social media boosting in order to reach more voters. In recent months, Common Cause staff in Texas has created materials regarding voter data and data privacy, due to the Department of Justice's efforts to obtain voter data.

11. Common Cause staff in Texas regularly field questions from the public related to voter registration and elections. Staff members have received questions regarding voter data and privacy and the State's data-sharing with the federal government.

12. Another way in which Common Cause increases voter participation in Texas is through voter registration efforts. For example, Common Cause staff encourage Democracy Fellows to complete the training and registration process needed to become deputy registrars, so that they can register voters at community and tabling events.

13. Election Protection is one of Common Cause's main programs in Texas. Common Cause staff members work with partner organizations to recruit and train volunteers to be poll observers. Volunteers are given an overview of voting rights, problems that may arise during an election, and the mission of the program. Poll observers are trained to spot issues, assist voters, and refer questions to a voter assistance hotline—the assistance may include helping to make sure voters are registered to vote and are at the right polling location.

14. Common Cause staff is aware that the Department of Justice has entered into a memorandum of understanding with the State of Texas, and that under the agreement, the Department of Justice intends to analyze Texas's voter file and then direct the State to remove

voter registrations for individuals identified as ineligible by the Department of Justice within 45 days.

15. The Department of Justice's attempt to gather voter data and nationalize voter registration interferes with Common Cause's election protection work in several ways. For one, Common Cause staff anticipate having to create materials concerning data and privacy issues because federal actions with regards to voter data have generated increased public attention and interest in those questions. Furthermore, because of the risk that voter registrations may be purged or deactivated as a result of the Department of Justice's collection of voter data, Common Cause staff in Texas anticipate having to conduct more intensive public education efforts, including by starting such campaigns earlier, to remind voters to check their registration status. Planning for public education efforts for a major general election typically begin at least a year out with Common Cause staff and coalition partners discussing and planning out what our program will look like, how many volunteers we'll need, what jurisdictions we'll prioritize, and what, if any, major changes need to be made to trainings and/or materials. Public-facing education typically would not begin until after we have concluded any elections that occur earlier in the calendar. However, this year, we've already started some educational efforts regarding privacy, including an informational video posted on social media, which is not a thing we'd normally do at this point in the election cycle. Had DOJ disclosed information about its collection and use of voter data earlier, we could have already begun training our volunteers and educating voters on those issues. Because we have already begun our voter education efforts, any further delay reduces the amount of time we have to inform the public about DOJ's actions and its impact on voters.

16. In order to accurately inform partners and voters, it is important that Common Cause has access to complete and accurate information about the processes and procedures related to voting and elections. Unless we obtain full and accurate information from the Department of Justice about its intended uses of voter data, the security of the agency's data practices, the persons that have access to Texas voters' data, and the process for removing Texas voters' registrations, we face a significant risk of misinforming voters and the broader public. Providing incorrect information to voters, volunteers, partner organizations, or the public in general could lead to disenfranchisement and would likely damage Common Cause's good will and reputation, which the organization has worked hard to build up and maintain for years.

17. Common Cause staff will also have to train volunteer poll observers to try to identify and assist voters who are unable to vote because their voter registration has been purged or deactivated as a result of the Department of Justice's actions. Our training currently runs about 90 minutes and we aim to have it cover only the essential procedural things volunteers need to know to perform their functions plus a very high-level overview of the top ten or so basic problems/questions they are most likely to encounter. We are already planning to make modifications to this training, and adding in new details and/or guidance because of the state's collaboration with DOJ interferes with our ability to minimize the length of the training and the burden on volunteers. We also often train Fellows or new Organizers to conduct these trainings but the more complex it becomes, the more likely it will be that more senior staff will have to conduct, or at least be present, on the trainings.

18. Common Cause has limited resources in Texas. There are only four permanent staff members to address all of the issues related to democracy and good government in one of the largest states in the country, in terms of both geography and population. Because of those

resource constraints, when an unexpected change to election and voting procedures occur, Common Cause staff must divert staff time and resources from other priorities in order to respond. For instance, in summer 2025, Common Cause staff had been planning to conduct a campaign related to election administration around the State by surveying election administrators and pursuing reforms—but due to Texas’s unexpected attempt to redraw congressional districts in a way that violated Common Cause’s fair redistricting criteria, staff had to pivot to opposing the redistricting effort instead.

19. In response to past efforts by Texas to purge voters, including through the use of the federal SAVE database, Common Cause has had to respond by engaging in public education to raise awareness about the potential erroneous removal of voters, including by preparing for and testifying at legislative hearings, contacting reporters and media about the issue, encouraging people to check their registrations, raising and explaining the issue on calls with other organizations, promoting the issue on social media, and working with coalition groups to try and identify and contact impacted individuals. Previous purges based on similar data incorrectly flagged up to 95,000 voters. Those past efforts occurred at a time when Common Cause Texas consisted of two staffers and their work described above consumed the vast majority of their time for nearly the entirety of the 2019 legislative session, from mid-February through the end of May when the session concluded, plus a great deal more time addressing lingering confusion for the remainder of that election cycle up until the 2020 General Election. In the event of another erroneous purge, Common Cause would have to attempt outreach to massive numbers of Texans to clarify their eligibility, significantly reshaping our work plan and capacity. Purging of qualified voters and deterring political participation undermine Common Cause’s mission and make our work of engaging voters less effective.

20. Unless the Department of Justice's implementation of its agreement with Texas is stopped, Common Cause will have to expend resources to engage in similar efforts to protect voters from being erroneously purged. Doing so will divert resources from Common Cause's other planned activities in Texas, including its advocacy efforts and its pursuit of election reforms at the local and county level. Other projects, such as advocating for fair redistricting at the local and county levels or working with county officials to encourage them to adopt educational resources and trainings modules on election administration will suffer and/or be delayed indefinitely if we have to shift focus to voter education efforts.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and that this Declaration was signed in Buda, TX, on May 15, 2026.

A handwritten signature in black ink, appearing to read 'Anthony Gutierrez', with a long horizontal flourish extending to the right.

ANTHONY GUTIERREZ

Exhibit G

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

vs.

Case No. 1:26-cv-01352-SLS

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

DECLARATION OF ANTHONY NEL

I, Anthony Nel, declare as follows:

1. I am over 18 years old and a member of Common Cause of Texas. The statements made in this declaration are based on my personal knowledge, information, and belief. I submit this declaration in support of Plaintiffs' motion for summary judgment.

Background

2. I have been a United States citizen since 2013.
3. I was born in Port Elizabeth (Gqeberha), South Africa, in 1996. I immigrated to the United States with my parents in 2004, when I was eight years old.
4. I was issued a Social Security Number ("SSN") and card in 2012, when I was fifteen years old. When I applied for an SSN, I was a lawful permanent resident.
5. My parents became naturalized U.S. citizens in March 2013, when I was sixteen years old. I automatically became a U.S. citizen when my parents naturalized.
6. I was issued a U.S. passport, confirming my U.S. citizenship, on July 17, 2013.
7. To my knowledge, the Department of Homeland Security ("DHS") has never issued me a Certificate of Citizenship, nor have I applied for one.

8. After becoming a U.S. citizen, I knew I would be entitled to vote when I turned 18 and felt that it was important to vote because it is a fundamental right of U.S. citizenship.

9. After turning 18, I registered to vote and began voting in state and federal elections in Texas. I first voted in the 2016 election and have voted eight times since then.

10. I currently live in and am registered to vote in Texas. In order to register to vote in Texas, I provided my name; date of birth; residential address; driver's license number or last four digits of my SSN; and telephone number.

11. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.

12. I voted in the March primary and intend to vote in the November midterm elections in Texas this year.

DHS's Expanded SAVE System Led to the Cancellation of My Voter Registration and Other Burdens on My Voting Rights

13. After voting in the November 2025 election (during the early voting period), I received a letter from the Denton County Voter Registrar, dated October 21, 2025, titled "Notice to Registered Voter for Proof of Citizenship (USCIS Verification)." A true and correct copy of the letter and accompanying envelope, with certain private information redacted, is attached hereto as Exhibit 1.

14. The letter states in part that a "comparison of the information in your voter registration records with the United States Citizenship and Immigration Services SAVE records show that you were not a United States citizen at the time of the comparative process." It then instructs: "[t]o maintain your active voter registration status, please provide proof that you are a United States citizen." The letter lists several types of documents that will be accepted as proof of U.S. citizenship, and notes that copies of the documents can be delivered by hand, mail, fax,

email, or any other method of transmission.

15. The letter further states: “Please provide proof of U.S. citizenship within (30) days from the date of this letter. If we do not receive a response from you within thirty (30) days, your voter registration will be cancelled.”

16. The exterior of the envelope in which the letter was enclosed had no markings indicating it was official election mail or that the enclosed letter had any bearing on my voter registration.

17. Upon reading the October 21 letter, I was shocked to learn that DHS’s SAVE system indicated I was not a U.S. citizen. As stated above, I have been a citizen with a U.S. passport since 2013. I was worried that the letter was part of a voter suppression effort to discourage Texans from exercising their right to vote, which I found deeply troubling as an ardent supporter of voting rights. I was also worried about the steps that I needed to take to ensure my voter registration would not be wrongly cancelled ahead of the approaching March 2026 primary election.

18. Of the documents sufficient to prove citizenship listed in the letter, the only document I have is a U.S. passport. However, my passport expired on July 17, 2023. Due primarily to the threat of my voter registration being cancelled unless I provided proof of citizenship, I applied to renew my passport and obtained a renewed passport on December 10, 2025.

19. While awaiting my renewed passport, I was worried that my voter registration would be cancelled improperly on the grounds that I am not a U.S. citizen, even though I am a citizen. So I began regularly using Denton County’s online voter lookup system to check my voter registration status.

20. In early December 2025, I checked Denton County's voter lookup system and saw that it no longer listed me as a registered voter.

21. On December 3, I emailed the Denton County Voter Registrar asking why my voter registration was cancelled.

22. On December 4, the Denton County Elections Administrator responded by email that my "name appeared on a list of potential non-citizens that was sent to us from the Secretary of State's office. On 10/22/2025 we mailed a letter to you asking for proof of citizenship. ... When you did not reply to the letter within the 30-day period, your registration was cancelled. ... If you can provide proof of citizenship with one of the documents listed in the letter, we can reinstate your registration. You can email documentation to this address."

23. I responded by email the same day, noting I am a U.S. citizen and that I intended to provide my passport in person prior to the March primary election. I also requested a copy of my voter history for Denton County, which a county employee provided. My voter history showed that my voter registration had changed on November 24, 2025, which I understood to mean it was cancelled on that date.

24. Although Denton County stated I could send documentary proof of my citizenship by email, mail, or fax, I am not comfortable doing so due to the data security and privacy risks of sending pictures of my sensitive personal documents, including my passport, by email or other unsecure methods of communication. Absent a reliable method of secure transmission, I am only comfortable providing this documentation in person.

25. Later in December, I received another letter from the Denton County Voter Registrar, postmarked December 3, 2025, titled "Notice of Cancellation." A true and correct

copy of the letter and accompanying envelope, with certain private information redacted, is attached hereto as Exhibit 2.

26. The letter states that my voter registration was cancelled on December 1, 2025, for “[f]ailure to respond to Notice for Proof of Citizenship,” and that I could request a hearing on the cancellation.

27. On or about December 16, 2025, I received my renewed passport.

28. On or about February 2, 2026, I provided the Denton County Voter Registrar with a copy of my renewed passport in person, and on March 3, 2026, I received verification that my voter registration was reinstated.

The Department of Justice Is Collecting, Disclosing, and Repurposing My Personal Data Without My Consent, Causing Me Distress and Risking Burdening My Fundamental Right to Vote

29. After my voter registration was cancelled, I learned more about DHS’s SAVE system and the Department of Justice’s (“DOJ’s”) efforts to compile every state’s and Washington D.C.’s voter rolls in service of creating a nationwide voter roll list and using states’ voter tolls to conduct voter roll list maintenance.

30. I learned that, in 2025, DHS expanded the SAVE system by allowing bulk searches of Americans’ personal data housed at the Social Security Administration (“SSA”), using only a name, date of birth, and SSN.¹ I also learned that the Texas Secretary of State had announced in a press release on October 20, 2025, that her office had used this new functionality to run Texas’s entire voter registration list with more than 18 million voters through the expanded SAVE system, that they identified “2,724 potential noncitizens” who were registered

¹ <https://www.uscis.gov/save/current-user-agencies/guidance/voter-registration-and-voter-list-maintenance-fact-sheet>; <https://www.federalregister.gov/documents/2025/10/31/2025-19735/privacy-act-of-1974-system-of-records>.

to vote in Texas, and that they referred those individuals to Texas counties (including Denton County) to determine their eligibility to vote.² The Secretary further stated that once the counties complete this process, “individuals who are deemed noncitizens that voted in a Texas election will be referred to the Office of the Attorney General” for investigation.

31. Based on the Texas Secretary of State’s October 20 press release and the October 21 letter I received from Denton County, it is my understanding that I am one of the “2,724 potential noncitizens” identified through DHS’s expanded SAVE system.

32. It is my understanding that, as part of the process of bulk uploading Texas’s entire voter registration list into SAVE, the Texas Secretary of State disclosed, at a minimum, my name, date of birth, and either my driver’s license number or last four digits of my SSN to DHS, and that this information will be retained in SAVE for at least 10 years. It is my understanding that after the Texas Secretary of State uploaded my voter registration information into DHS’s SAVE system, DHS disclosed that information to SSA so that SSA could match it against its own records about me.

33. It is my understanding, based on the Texas Secretary of State’s October 20 press release and Denton County’s October 21 letter to me, that SAVE could not confirm my U.S. citizenship due to outdated, inaccurate SSA citizenship data queried by SAVE using my SSN, as well as SAVE’s new functionality allowing bulk queries of state voter rolls. As a result, my understanding is that SAVE returned my case to the Secretary to seek documentary proof of citizenship directly from me. This led to Denton County demanding that I provide documentary proof of citizenship within 30 days and then, when I was unable to do so, cancelling my voter registration. Absent the SAVE expansion and its new bulk search-by-SSN functionality, it is my

² <https://www.sos.state.tx.us/about/newsreleases/2025/102025.shtml>.

understanding that these events would not have occurred and my voter registration would not have been cancelled.

34. Because Denton County cancelled my voter registration for lack of proof of citizenship, I felt pressured to provide proof of citizenship not only to ensure I could exercise my right to vote in the March 2026 primary election and future elections, but also to avoid the possibility that the Texas Secretary of State will, consistent with the process outlined in her October 20 press release, refer me to the Texas Attorney General for (unwarranted) investigation based on my prior voting, even though I did so lawfully as a U.S. citizen.

35. It is my understanding that the Texas Secretary of State, after executing a Memorandum of Understanding with DOJ similarly provided DOJ with Texas's entire voter registration list as part of the DOJ's efforts to compile voter data from all 50 states and the District of Columbia. It is my understanding that the voter list Texas sent to DOJ included information such as my name, date of birth, address, driver's license number, and SSN.

36. I have not consented to, and do not consent to, the Texas Secretary of State disclosing the information about me that her office shared with DOJ. I provided that information for use by state and local Texas officials, not to be uploaded into a national voter database at DOJ or national citizenship database housed at DHS. I expected that information—especially my driver's license number and SSN—to remain private and protected by state and local Texas officials.

37. It is my understanding that DOJ intends to disclose the voter registration lists it collects from the states—including Texas—to DHS so that it can run the data through the SAVE system. It is my understanding that the DOJ MOU requires Texas to remove any voters DOJ

identifies as ineligible to vote from Texas's voter roll. I also have not consented to, and do not consent to, DOJ disclosing that information with DHS through the SAVE system.

38. It is also my understanding that the DOJ MOU allows the DOJ to disclose personally identifiable information ("PII") to private contractors to assist with list maintenance verification. It is not clear to me what "list maintenance verification procedures" are, or who these contractors might be. I never consented to, nor do I consent to, DOJ sharing my personal information with anyone outside of the government.

39. I am disturbed, uneasy, anxious, and frustrated that the government has violated my trust by collecting, disclosing, matching, and repurposing my personal information without my consent in an effort to create a national database of voters. I am also worried that DOJ may be seeking to create a new, comprehensive list of voters who were born abroad in order to target, surveil, or simply make life harder for foreign-born American citizens. This makes me feel like I am living in a surveillance state where government actors can access my most private information at will. I expected the United States to respect all of its citizens' privacy, but instead I am opposing government efforts to create a centralized profile on me, including my sensitive information, for a national voter database.

40. I am also concerned that by collecting voter data from many different states, DOJ is incentivizing hackers or bad actors to try to gain access to data that is otherwise maintained in a decentralized manner by each individual state. My concerns are amplified by my knowledge of the current administration's history of misusing and failing to protect personal data.

41. Because DOJ intends to share my sensitive personal information across federal agencies and with private contractors, I am also deeply worried that my data will be stored or transferred in an unsecured manner, exposing me to a data breach and identity theft and fraud. I

am especially concerned about the unsecured storage or transfer of files containing information such as my full name, date of birth, address, driver's license number, and SSN, because the exposure of those data elements in tandem creates a heightened risk of identity theft and fraud. This fear is especially heightened by the DOJ's purported authority to share such sensitive personal information with third-party contractors outside of the government, as outlined in its MOU with Texas.

42. I deeply value and cherish my right to vote. I am greatly concerned that I will be purged from the voter rolls again based on Texas sharing my voter data with DOJ and the statements in the DOJ MOU suggesting Texas is required to "clean" its voter rolls based on DOJ identifying purported voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns. I am also greatly concerned that I will be wrongly investigated by DOJ or other federal agencies based on DOJ's review of Texas's voter rolls.

43. I am particularly worried because DOJ intends to rely on or is already relying on SAVE and SSA citizenship data, which I have personally confirmed is inaccurate and out of date for me. In December 2025, I called SSA and was informed by an SSA employee that I am (incorrectly) listed as a non-citizen in SSA's records. That was not surprising to me, because the only prior time I had interacted with SSA was when I obtained a Social Security card in 2012, before I became a U.S. citizen. To my knowledge, there is no requirement for me to update my citizenship status with SSA, and I have not done so.

44. Texas has already incorrectly removed me from the voter rolls once using inaccurate information from SAVE and SSA records. It is my understanding that DOJ is referring the purported noncitizen voters it identifies to Homeland Security Investigations, and I

am extremely worried about being wrongly investigated because of DOJ relying on inaccurate information that wrongly suggests I am a noncitizen voter.

45. I fear that I will be forced to prove my citizenship status again and am distressed that I have to remain vigilant about my voter registration status. I plan to continue voting regularly, and as long as Texas and DOJ intend to use the expanded SAVE system and the unreliable data it utilizes, I will feel compelled to continue regularly checking my voter registration status to ensure it is not wrongly cancelled again.

46. It is my understanding that, based on the previous SAVE search of my personal information, SSA has already returned a response to DHS that included my SSN, name, date of birth, an indicator of my citizenship status, and other information that SSA collected when I applied for a Social Security card in 2012. It is my understanding that my personal SSA data will be retained in DHS's SAVE system for at least 10 years.

47. I have not consented to, and do not consent to, SSA disclosing and verifying my personal information from SSA records to DOJ, DHS, or any other federal, state, or local agency to run citizenship checks for voter list maintenance or any other purpose. I expected that data to remain private within SSA and be used only for purposes consistent with why SSA collected the data, such as to determine eligibility for SSA benefits or authorization to work in the U.S. I never expected my personal SSA information to be disclosed to DOJ, DHS, or any other federal, state, or local agency for use in a massive national citizenship database for voter eligibility checks.

48. I am distressed by the fact that the government has repurposed my sensitive SSA data without my consent to determine my eligibility to vote, when the information is not suitable for that purpose and was never intended to be used in that way.

49. These fears were only heightened when I learned that the Texas Secretary of State recently executed the DOJ MOU to share Texas's voter registration data with DOJ and to surrender its voter list maintenance responsibilities to the federal government.

50. I am also worried that, even though I provided Denton County with documentary proof of citizenship and my voter registration was reinstated, DOJ will continue to wrongly identify me as a non-citizen based on faulty underlying data when DOJ runs bulk voter roll searches in the future, and that I will again be forced to prove my citizenship status in order to retain my voter registration. Being caught in such a cycle, with my voting rights on the line, is distressing to me.

51. The privacy of my personal information—including the data contained in my voter file—is very important to me. From a young age, my parents instilled in me the importance of protecting the confidentiality of my personal information such as my SSN and driver's license number, and so I have always treated my Social Security card and driver's license as ultra sensitive documents. Moreover, because I pay taxes and plan to retire and receive Social Security benefits in the future, SSA has personal information about me that I consider highly sensitive. I have trusted SSA and Texas election officials to keep my information private and only use it for lawful purposes. I understood them to be bound by laws that would keep them from sharing this information across government agencies for completely unrelated purposes. I did not consent to them sharing this highly sensitive information with the federal government for unlawful or undisclosed purposes.

52. It is extremely concerning that so many people across all levels of government have access to my personal data without my consent. I am skeptical of any unauthorized national database, but especially one that contains my private data and lets government officials access

and utilize it in a way that can be used against me and others similarly situated.

53. Beyond feeling violated by the disclosure of my personal information, I also feel scared. As described above, I question how secure my information is. I do not know who can access my data, and I fear that my information may be weaponized against me for political retribution or other improper purposes.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 14, 2026, in Texas.



Anthony Nel

Exhibit 1



DENTON COUNTY
ELECTIONS ADMINISTRATION

FRANK PHILLIPS, CERA
Elections Administrator

BRANDY GRIMES, CERA
Deputy Elections Administrator

Denton County Voter Registrar
Mailing Address: 701 Kimberly Dr., Ste. A100, Denton, TX 76208
Phone Number: (940) 349-3200
Fax Number: (940) 349-3201
Email Address: Elections@DentonCounty.gov
Website: www.votedenton.gov

10/21/2025
ANTHONY K. NEL

DENTON, TX

NOTICE TO REGISTERED VOTER FOR PROOF OF CITIZENSHIP (USCIS VERIFICATION)

Dear ANTHONY K. NEL :

As the voter registrar for Denton County, I am writing to notify you of important information regarding your voter registration.

You are currently registered to vote in this county. We have received information from the Texas Secretary of State reflecting that you might not be a United States citizen. A comparison of the information in your voter registration records with the United States Citizenship and Immigration Services SAVE records show that you were not a United States citizen at the time of the comparative process. Although you can obtain United States and state government identity documents as a non-United States citizen, only United States citizens are eligible to vote.

To maintain your active voter registration status, please provide proof that you are a United States citizen. Proof of United States citizenship can be established by presenting a copy of any of the following documents:

- U.S. birth certificate or a Consular Report of Birth Abroad of a Citizen of the United States issued by the United States Department of State;
- United States passport;
- Certificate of Naturalization or Certificate of Citizenship; or
- Your parent's Certificate of Naturalization along with your birth certificate if you became a U.S. citizen as a result of your parent's naturalization.

There are several ways to provide proof of U.S. citizenship to my office. You can deliver it by hand, or you can send it by mail, fax, electronic mail, or any other method of transmission. My office's contact information is listed at the top of this letter.

Please provide proof of U.S. citizenship within thirty (30) days from the date of this letter. If we do not receive a response from you within thirty (30) days, your voter registration will be cancelled.

In the event that your registration is cancelled, you can still be immediately reinstated by providing proof of U.S. citizenship to my office or at your polling location, even if the thirty (30)-day period has already passed. You may also request a hearing to challenge your cancellation, even if you do not possess one of the above forms, by contacting my office.

If you have any questions regarding this notice or your voter registration, please contact my office at (940) 349-3200.

Signature of Voter Registrar

10-21-2025

Date



DENTON COUNTY
ELECTIONS ADMINISTRATION

FRANK PHILLIPS, CERA
Elections Administrator

BRANDY GRIMES, CERA
Deputy Elections Administrator

Registrador de Votantes del Condado de Denton
Mailing Address: 701 Kimberly Dr., Ste. A100, Denton, TX 76208
Phone Number: (940) 349-3200
Fax Number: (940) 349-3201
Email Address: Elections@DentonCounty.gov
Website: www.votedenton.gov

10/21/2025
ANTHONY K. NEL

DENTON, TX

**AVISO AL VOTANTE REGISTRADO PARA PRESENTAR PRUEBA DE SU CIUDADANÍA
(VERIFICACIÓN DE USCIS)**

Estimado ANTHONY K. NEL ,

Como el Registrador de Votantes del Condado de Denton, me comunico con usted para hacerle llegar información importante con respect a su registro electoral.

Usted está actualmente registrado para votar en este condado. Hemos recibido información de la Secretaría de Estado de Texas que refleja que usted podría no ser un ciudadano de los Estados Unidos. Una comparación entre la información de su registro de votante y los registros del Sistema SAVE del Servicio de Ciudadanía e Inmigración de los Estados Unidos (USCIS) indica que usted no era ciudadano estadounidense en el momento del proceso comparativo. Aunque puede obtener documentos de identidad del gobierno de los Estados Unidos y del estado como ciudadano no estadounidense, solo los ciudadanos estadounidenses tienen derecho a votar.

Para mantener su estado de votante registrado activo, le solicitamos que nos proporcione prueba de que usted es un ciudadano de los Estados Unidos. La prueba de la ciudadanía de los Estados Unidos se puede establecer presentando una copia de cualquiera de los siguientes documentos:

- Certificado de nacimiento estadounidense o Certificado consular de nacimiento en el extranjero emitido por el Departamento de Estado de los Estados Unidos;
- Pasaporte estadounidense;
- Certificado de naturalización o Certificado de ciudadanía; o
- Certificado de naturalización de su padre o madre junto con su Certificado de nacimiento, si se convirtió en ciudadano estadounidense como resultado de la naturalización de su padre o madre.

Hay varias maneras de proporcionar la prueba de su ciudadanía estadounidense a mi oficina. Puede traerla personalmente, enviarla por correo, fax, correo electrónico o por cualquier otro método de transmisión. La información de contacto de mi oficina se detalla al principio de esta carta.

Favor proporcionar la prueba de su ciudadanía estadounidense dentro de los treinta (30) días a partir de la fecha de esta carta. Si no recibimos una respuesta dentro de los próximos treinta (30) días, su registro electoral será cancelado. Si su registro electoral se cancela, puede reinscribirse inmediatamente al presentar la prueba de su ciudadanía estadounidense en mi oficina o en el lugar de votación que le corresponde, aún después del plazo de treinta (30) días. También puede solicitar una audiencia para impugnar la cancelación, incluso si no posee uno de los documentos anteriores, comunicándose con mi oficina.

Si tiene alguna pregunta con respecto a este aviso o sobre su registro electoral, comuníquese con mi oficina al (940) 349-3200.

Firma del Registrador de Votantes

10-21-2025

Fecha

Elections Administrator
Denton County
PO Box 1720
Denton, TX 76202

Presort
First Class Mail
ComBasPrice



US POSTAGE PAID BY PITNEY BOWES



ZIP 76208 \$ 000.68⁶
02 4W
0000385099 OCT 22 2025

1215912714 106201
ANTHONY K NEL
[REDACTED]
DENTON TX [REDACTED]

020 I IL-AMP 76209

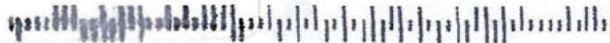


Exhibit 2

21-48
Prescribed by Secretary of State
Sections 16.031(a), 16.036, Texas Election Code
9/2023

Name: ANTHONY K. NEL

VUID: [REDACTED]

NOTICE OF CANCELLATION

Notice is hereby given that your voter registration has been cancelled in Denton County on

12-1-25

(Date)

The reason for cancellation was:

Check one:

- Receipt of request to cancel voter registration.
- Receipt of abstract of total mental incapacity or partially mentally incapacitated without the right to vote.
- Receipt of abstract of felony conviction.
- Receipt of abstract of judgment in an election contest that you were a disqualified voter.
- After examination of your registration under Sec. 16.033, Texas Election Code.
- Notice was received from the Secretary of State that you are currently registered to vote in another Texas county.
- Failure to respond to Notice for Proof of Citizenship.

I received a change of address which indicated a new address outside this county. You will need to re-register in the county of your new address. Your registration is cancelled in this county.

You may request a hearing on the cancellation of your registration by submitting a written request for such hearing. If you request a hearing, a notice will be mailed to you setting forth the date of the hearing. The hearing will be scheduled within ten (10) days after your request or on a later date if you so request.

If after the hearing, the voter registrar determines that your registration shall remain cancelled, you are entitled to appeal the adverse decision issued by the voter registrar by petitioning for review in district court not later than the 30th day after the adverse decision is issued.

If you should have any questions regarding this cancellation, please contact me at (940) 349-3200.

Frank Phillips
Signature of Voter Registrar

701, Kimberly Dr., Ste. A100, Denton, TX 76208
Address of Voter Registrar

21-48
Prescribed by Secretary of State
Sections 16.031(a), 16.036, Texas Election Code
9/2023

Name: ANTHONY K. NEL

VUID: [REDACTED]

AVISO DE CANCELACIÓN

Por este medio se le notifica que con fecha de 12-1-25 se ha cancelado su inscripción electoral
(fecha)
en el Condado de Denton.

El motivo de dicha cancelación fue el siguiente:

Marcar una de las razones a continuación:

- Se recibió una petición para cancelar su inscripción.
- Se recibió el sumario de un fallo de incapacidad mental total o incapacidad mental parcial sin el derecho al voto.
- Se recibió el sumario de una convicción de delito grave.
- Se recibió el sumario referente a una disputa electoral en la que usted quedó descalificado/a como votante.
- Después de haber revisado su inscripción electoral bajo la Sección 16.033 del Código Electoral de Texas
- Se recibió un aviso de la Secretaría del Estado indicando que usted actualmente se encuentra inscrito/a en otro condado de Texas, para votar.
- No se recibió respuesta al Pedido de Comprobante de Ciudadanía.
- He recibido un aviso de su cambio de domicilio a una nueva dirección fuera de este condado. Tendrá que volver a inscribirse en el condado donde se ubica su nueva dirección. Por ende, queda cancelada su inscripción en este condado.

Si desea una audiencia con respecto a la cancelación de su inscripción electoral, podrá pedirla por escrito. Si pide una audiencia, se le enviará por correo el aviso correspondiente comunicándole la fecha de la audiencia, misma que se llevará a cabo, en un plazo de 10 días después de haberla solicitado o, a petición suya, en fecha posterior.

Si al concluirse la audiencia el Registrador de Votantes resuelve que la cancelación de su inscripción deberá permanecer en vigor, usted tendrá el derecho de apelar la decisión contraria del Registrador de Votantes mediante petición de revisión judicial ante un tribunal de distrito, en un término no mayor de 30 días a partir de la fecha de emisión de la decisión contraria.

Si tiene alguna pregunta referente a esta cancelación, sírvase comunicarse conmigo llamando al (940) 349-3200.

Frank Phillips

Firma del Registrador de Votantes

701 Kimberly Dr., Ste. A100, Denton, TX 76208
Dirección del Registrador de Votantes

Elections Administrator
Denton County
PO Box 1720
Denton, TX 76202

Presort
First Class Mail
ComBasPrice



US POSTAGE TM PITNEY BOWES



ZIP 76208 \$ 000.68⁰
02 4W
0000385099 DEC 03, 2025

1215912714 106201

ANTHONY K NEL

DENTON TX

20

KJLDIMP

76209

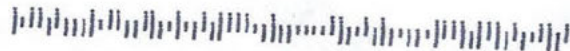


Exhibit H

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF LINDA DUCKWORTH

I, Linda Duckworth, declare as follows:

Background

1. I am over the age of 18. The statements made in this declaration are based on my personal knowledge, information, and belief.
2. I currently live in Omaha, Nebraska.
3. I am a member of Common Cause of Nebraska.
4. I legally changed my name in 1976 in Missouri when I got married.
5. I was born in 1952 and have been a United States citizen since my birth.

Voting History

6. I currently live in and am registered to vote in Douglas County, Nebraska. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.
7. I have been registered to vote in Nebraska since I moved here in 2004. Before that I was registered to vote in Missouri.

8. In order to register to vote in Nebraska, I provided the following information: name, date of birth, residential address, mailing address, address of last registration, driver's license number or last four digits of my Social Security number, telephone number, place of birth, email address, date of application for registration, and party affiliation.

9. I consider this information to be highly private, especially my party affiliation. When I provided this information to the state of Nebraska, I provided it solely to exercise my fundamental right to vote and expected this information to stay private.

10. I have not consented to my information being obtained, stored, or used by the federal government. And I have not consented to the federal government sharing my information with private contractors or other third parties.

11. I deeply value the right to vote and view voting as not only a right but a privilege. I strongly believe that it is important to be knowledgeable about those who are running for office and the issues they stand for. I also ran for a nonpartisan office in 2018.

12. I particularly value my right to vote as, when I was in college, young people my age who were dying in Vietnam did not have the right to vote. I was 19 years old the year that the Constitution was amended to lower the voting age to 18. Ever since we received the right to vote, exercising that right has been deeply meaningful to me.

13. I first registered to vote in 1972 and have kept my voter registration current ever since.

14. I have voted regularly since 1972 and intend to continue doing so, including in all upcoming local, state and federal elections in Nebraska this year.

15. Encouraging civic participation is very important to me. I am a committee chair for the League of Women Voters for Nebraska ("LWVNE"), and served as president of the

LWVNE from 2012 to 2014. In those roles, I led many discussions about voting, including presenting on the history of voting while in costume as Susan B. Anthony. I also served as president of the League of Women Voters of Greater Omaha from 2007 to 2011. During that time, I led the expansion of the organization's voter registration efforts into high schools and to naturalization ceremonies. I have participated in many voter registration events, including the naturalization ceremonies, and every time it fills me with pride to see newly registered voters realizing the solemn duty they have to participate in our democracy in this way.

16. I regularly encourage and register people in my community to vote. The League of Women Voters publishes a voter guide, both in print and online, posing questions to the candidates that voters may find helpful as they consider the ballot. I do my part to distribute this information and to represent the League by speaking to groups about voting. I intend to continue with that work between now and the general election in November.

Voting Concerns

17. It is my understanding that the Nebraska Secretary of State has provided the U.S. Department of Justice ("DOJ") with Nebraska's entire voter registration list as part of the DOJ's efforts to compile state voter data.

18. I am concerned that DOJ may incorrectly identify me as ineligible to vote and instruct Nebraska to cancel my registration. People born before 1981, as I was, and those who have legally changed their names, as I have, are at heightened risk of such misidentification.

19. I am concerned about DOJ's collection of not only my own voter registration data, but also the data of other people that I care about. In particular, I am concerned about people I know who are naturalized citizens or who were convicted of a felony, as I understand

that they are also at a heightened risk of being incorrectly identified by DOJ as ineligible voters. My concern for the people I care about impacts me as well.

Privacy Concerns

20. I do not trust DOJ with this personal data. I am deeply concerned about this administration's ability to protect my personal data.

21. My concerns are amplified by my knowledge of the current administration's history of misusing and failing to protect personal data in ways that are illegal and unethical.

22. I am aware that employees of the U.S. Department of Government Efficiency, for example, failed to properly safeguard private individuals' highly sensitive personal information. This makes me more uncomfortable with this DOJ having my information. I fear that this DOJ will act as if there are no restrictions on their use of this data.

23. Further, I am concerned about the potential that DOJ may disclose my personal information to external parties and I feel threatened by the possibility of that occurring.

24. I am especially sensitive about potential threats to the security of my private, personal information because I have been targeted by attempted identity thieves in the past. In 2019, someone unsuccessfully attempted to impersonate me and steal my Social Security number. Since that experience, I have been very conscious of my information security, and I take the steps I can to safeguard my personal information. I am very concerned that the government is not helping with those safeguards.

Informational Injury

25. I did not have an opportunity to comment on DOJ's collection and use of my voter registration data. Had I been given the opportunity to comment, I would have done so.

26. When I learned of DOJ's requests for Nebraska's voter registration data, I submitted a comment to Nebraska's Secretary of State requesting that Nebraska not share this information with DOJ. I did not receive a reply.

27. I have previously voiced my concerns about what the government is doing in regards to elections. Between 2011 and 2022, I testified to the Nebraska Legislature a number of times regarding voting. My message always centered on safeguarding citizens' right to the ballot. It never occurred to me to worry about safeguarding the private information contained in voter registrations. I had immense trust in our county's election commission and in the Nebraska Secretary of State to keep that information safe. I do not have the same trust in the federal government.

28. I want to know what the federal government is doing with my voter registration data and am concerned that I do not have this information.

29. It is extremely concerning that people across the government may have access to my personal data without my consent. I am skeptical of any unauthorized national database, but especially one that contains my private data and lets government officials access and utilize it in a way that can be used against me and others similarly situated.

30. Beyond feeling violated by the disclosure of my personal information, I also feel scared. As described above, I question how secure my information is. I do not know who can access my data, and I fear that my information may be improperly used against me.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 17, 2026, in Nebraska.

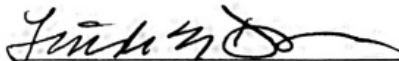

Linda Duckworth

Exhibit I

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF RUTH NASRULLAH

I, Ruth Nasrullah, declare as follows:

Background

1. I am over 18 years old. The statements made in this declaration are based on my personal knowledge, information, and belief.
2. I live in Houston, Texas.
3. I am a member of Common Cause of Texas.
4. I was born in 1961 and have been a United States citizen since my birth.
5. I have legally changed my name three times due to marriage. I first legally changed my name in 1983 after I married my first husband in New York State. I then legally changed my name in 1997 when I married my second husband in Nevada. I legally changed my name for a third time in 2003, when I married my current husband in Texas.

Voter Registration History and Voting Concerns

6. I currently live in and am registered to vote in Harris County, Texas. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.

7. I first registered to vote in 2004 and have kept my voter registration current ever since.

8. In order to register to vote in Texas, I provided the following information: name, date of birth, residential address, driver's license number or last four digits of my Social Security number, telephone number, gender, voter registration number, and indication of interest in serving as an election worker.

9. I provided this information to the state of Texas solely to exercise my fundamental right to vote.

10. I consider this information highly private. When I provided this information to the state, I did so in order to exercise my right to vote and I expected this information to remain private and securely protected. I believe that the data people share with the state for the purpose of registering to vote should not be used for any other purpose. I have not consented to my registration information being obtained, stored, or used by federal agencies. Nor have I consented to federal agencies sharing that information with private contractors or other third parties.

11. I deeply value my right to vote, and view voting as the hallmark of American democracy. Exercising my right to vote allows me to have power and participate in our government. I consider this right to be close to sacred.

12. I have voted regularly since 2004 and intend to continue doing so, including in all upcoming local, state, and federal elections in Texas this year.

13. Encouraging civic participation is very important to me. I am a certified volunteer deputy voter registrar in Harris County and Brazoria County, Texas. In this role, I help eligible residents register to vote and promote broader voter participation in my community.

14. Safeguarding voters' ability to participate in elections is equally important to me. I have worked as an election clerk and as an alternate election judge in Harris County in many elections over the past twenty years. I was appointed as a poll watcher in 2023 and have served in that role several times. And for approximately the last eight years, I have served as a volunteer for the Texas Election Protection program, which is run by a coalition of civil society groups including Common Cause.

15. It is my understanding that the Texas Secretary of State has provided the U.S. Department of Justice ("DOJ") with Texas's entire voter registration list as part of the DOJ's efforts to compile state voter data.

16. I am deeply concerned that the state of Texas and the federal government may be violating the law by sharing this information and using it inappropriately. Having served as an election clerk and as an alternate election judge, I understand firsthand how critical it is that election administration be conducted in strict accordance with the law.

17. I fear that this administration may make erroneous connections with my data that mistakenly result in my voter registration being terminated. I understand that there is a heightened risk of erroneous connections for those who, like me, have changed their legal names. I am concerned that, as a result of an error, the government may wrongly accuse me of being illegally registered to vote. Even if I could disprove that accusation, I would not want to have to fight it in court, and I would not want to be labelled a potential criminal.

Privacy Concerns

18. I feel that my privacy has been intruded on and my confidence breached by DOJ collecting my voter registration information. To the extent that DOJ is sharing my information

with the U.S. Department of Homeland Security (“DHS”) or private third-party contractors, that sharing further compounds the intrusion on my privacy.

19. I do not trust DOJ or DHS with this personal data, and I am deeply concerned about this administration’s ability to protect it. This concern is compounded because my Social Security account was already hacked last year, though I was able to recover my access and restore my account.

20. I also fear that this administration may deliberately misuse this data to target me. I am especially concerned about being singled out because I have a Muslim last name, and previously had a Palestinian last name for about 13 years. I also worked for the Council on American-Islamic Relations (“CAIR”) from approximately 2014 to 2017, and for the Texas chapter of a Muslim civic engagement group called EngageUSA for several months in 2020 and from 2023 to 2024. In addition to my paid work with these organizations, I have volunteered with them for many years. For these reasons, I fear that this administration may target me intentionally, either by revoking my voter registration or in some other manner I can’t predict. I have been deeply troubled by reports that this administration has unlawfully detained people, including Palestinian activist Leqaa Kordia. I understand that ICE arrested her during a lawful protest, like many protests I have attended over the years, and then detained her for a year, despite a court ordering ICE to release her three times. I do not trust the President, his administration, or the members of his party in Congress to follow the law and I fear similarly becoming a target of unlawful and unfounded persecution.

21. The possibility of being targeted by anyone—but particularly the federal government—causes me serious anxiety and distress. These feelings are compounded because I have been a target of harassment and violence before.

22. During my employment at CAIR, we routinely received phone calls threatening enough that we reported them to the FBI.

23. I was also physically attacked by an anti-Muslim agitator in 2015. CAIR had organized a Muslim community outing to the Texas State Capitol to promote civic education and to engage with elected officials. I was speaking on behalf of the organization on the Capitol steps when a woman came from behind, grabbed the microphone out of my hand, and began vilifying Muslims. Police were present but they did not immediately intervene. Another CAIR employee eventually recovered the microphone, but the woman remained throughout the event, repeatedly shouting anti-Muslim slurs. She was never arrested or removed.

24. I also received threats as a result of a blog I published on the Houston Chronicle's website about the experience of being an American Muslim. On one occasion, a commenter made a threat serious enough that the Chronicle's staff advised me to report it to the police. On another, a reader tracked down the bookstore where I worked at the time, came in, and announced that he did not like Islam. Although I was able to diffuse the situation by telling him that he was entitled to his opinion and offering him tea, it was deeply unsettling to know that he had sought me out in person to intimidate me. I also received anonymous letters by mail with threatening and hateful content.

25. My daughter and I were also subject to violence, stalking, and harassment by my ex-husband in the 1990s. After the glass window in the front door of our home was shattered, we stayed in a battered women's shelter until we could secure new housing. Although we obtained a restraining order, he violated it repeatedly, and he eventually served a year in prison. Those years taught me to be vigilant about my safety and privacy. As a result, I remain particularly sensitive to any erosion of the personal privacy and security that I fought so hard to establish.

26. I now choose to engage in public life and speak publicly about some aspects of my personal life, such as my religion. I am deliberate, however, about what I choose to share, disclosing details of my private life when I believe that doing so will advance a cause that I care about.

27. I am very aware of my personal security. For example, I use strong passwords and regularly change them, use Proton Mail for its encrypted email service, and never answer phone calls from unknown numbers.

28. I am deeply anxious and distressed knowing that sensitive personal information has been disclosed without my consent to DOJ and DHS, and that those agencies may share it further with other third parties. I find this particularly distressing because I fear that this administration may intentionally use that information to target me.

Informational Injury

29. I did not have an opportunity to comment on DOJ's collection and use of my voter registration data. Had I been given the opportunity to comment, I would have liked to do so.

30. I regularly voice my opinion about what the government is doing and have a history of commenting on government decisions. I regularly call and write to my local, state, and federal representatives. I have also testified several times at the Texas State Capitol, most recently about environmental regulations in 2025. And I regularly submit formal, written comments about proposed government actions. For example, last year I submitted written testimony to the Texas House of Representatives opposing HB 2988, which would have removed protections against frivolous lawsuits targeting journalists and others. I would have liked to comment on DOJ's actions here before it collected my voter registration data.

31. I want to know why the federal government is collecting voter registration information from the states, and if it has a compelling reason to do so. I also want to know how the federal government is using this information.

32. It is extremely concerning that people across the government may have access to my personal data without my consent. I am skeptical of any unauthorized national database, but especially one that contains my private data and lets government officials access and utilize it in a way that can be used against me and others similarly situated.

33. Beyond feeling violated by the disclosure of my personal information, I also feel scared. As described above, I question how secure my information is. I do not know who can access my data, and I fear that my information may be weaponized against me for political retribution or other improper purposes.

34. If I were registering to vote for the first time, knowing that my voter registration information would be shared with the federal government may have given me pause. However, I've been registered in Texas for many years, and this will not stop me from voting. I don't think anything could stop me from voting.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 15, 2026, in Texas.


Ruth Nasrullah

Exhibit J

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF HALEY SMITH

I, Haley Smith, declare as follows:

Background

1. I am over 18 years old. The statements made in this declaration are based on my personal knowledge, information, and belief.
2. I live in San Marcos, Texas.
3. I am a member of Common Cause of Texas. I am also the Vice Chair of Common Cause of Texas's Advisory Board.
4. I was born in 2004 and have been a United States citizen since my birth.
5. I am currently a student at Texas State University. Like many students, my residential address changes frequently.
6. I most recently moved in the summer of 2025, from another address in San Marcos, Texas. Prior to that, I moved in 2023 and 2022. I expect that I will move again this autumn, after I graduate from college.

Voting History

7. I currently live in and am registered to vote in Hays County, Texas. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.

8. I registered to vote in 2022, when I was 18 years old. At that time, I resided in my freshman year college dormitory.

9. I have regularly voted in local, state, and federal elections since I registered to vote, and I plan to continue to do so.

10. In order to register to vote in Texas, I provided the following information: name, date of birth, residential address, driver's license number, telephone number, gender, voter registration number, and indication of interest in serving as an election worker.

11. I provided this information to the state of Texas solely to exercise my fundamental right to vote.

12. I consider this information highly private. When I provided this information to the state, I expected this information to remain private and securely protected.

13. I have not consented to my information being obtained, stored, or used by the federal government, or to the federal government sharing my information with private contractors or other third parties..

14. I deeply value and cherish my right to vote. I believe that voting rights are fundamental to our democracy as the most powerful and direct method to participate in government and exercise fundamental rights. I am deeply alarmed to witness voting rights increasingly come under attack, and I am determined to do everything in my power to protect and preserve our democracy.

15. I first became involved with Common Cause as a Campus Democracy Fellow in 2022, during my freshman year of college. In that role, I became a certified voluntary registrar in Hays County and led civic engagement efforts on my campus and in my community, including voter registration and mobilization campaigns. I continued to promote Common Cause's civic engagement efforts throughout my four years in college, including by joining Common Cause of Texas's Advisory Board in 2024.

Voting Concerns

16. It is my understanding that the Texas Secretary of State has provided the U.S. Department of Justice ("DOJ") with Texas's entire voter registration list as part of the DOJ's efforts to compile voter data from all 50 states and the District of Columbia.

17. I feel that my right to vote is jeopardized by DOJ collecting my voter registration data.

18. I shared personal data with the state to register to vote and trusted the state to use it for that purpose alone.

19. I wish that I could say that I trust DOJ to use this personal data lawfully and appropriately, but I do not. I am also skeptical about the ability of this administration to use state voter data to correctly and responsibly identify ineligible voters.

20. I am deeply concerned about the prospect of being wrongly identified as an ineligible voter. I understand that individuals who have frequently changed their residential address are at an increased risk of being wrongly identified as ineligible to vote. I fear that, if that were to happen, I could be disenfranchised or even face baseless and unfounded criminal prosecution.

21. Even if I could successfully defend myself against a criminal prosecution, I do not want to have to do so, and I do not want the government to label me as a potential criminal.

22. Although DOJ's collection of the state's voter data would not stop me from voting, I believe that it will make others hesitate to register. I spend a lot of time and effort to convince people that their right to vote is important enough that they should register to vote, and based on my experience, I believe that this will be an obstacle that will make that work harder for me and others like me who are working to promote participation in elections.

Privacy Concerns

23. I am deeply concerned about DOJ's ability to protect my personal data. My concern is amplified by this administration's particularly checkered history with data security.

24. I am further concerned about the possibility of DOJ not only storing this information itself, but also sharing it with the Department of Homeland Security ("DHS") and third-party private contractors. I do not trust DHS employees or private contractors to access my private voter registration data safely and securely.

25. I believe that the federal government should be working to protect the people first and foremost, but I do not trust that this administration is doing so.

26. Personal privacy is particularly important to me because I am a gay woman and I have a transgender brother. We grew up in a very conservative area of Texas and encountered hostility on many occasions. I have concerns for my own physical safety and that of my family should the private, personal information contained in our voter registration files become public.

27. As a gay woman, I also fear that this administration may deliberately misuse this information against me.

Informational Injury

28. I did not have an opportunity to comment on DOJ's collection and use of my voter registration data. Had I been given the opportunity to comment, I would have liked to do so and let it be known that I do not want my voter registration data shared with the federal government.

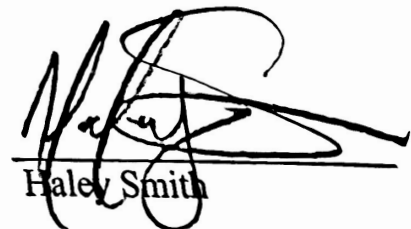
29. I regularly voice my opinion about what the government is doing and have a history of commenting on government decisions, including by offering testimony at the state legislature. For example, I have submitted written comments and testified at the Texas State Capitol.

30. I am anxious and concerned because I do not know what the government is doing with my data, or what steps it is taking to ensure that my data is protected. It is extremely concerning that people across the government may have access to my personal data without my consent. I am skeptical of any unauthorized national database, but especially one that contains my private data and lets government officials access and utilize it in a way that can be used against me and others similarly situated.

31. Beyond feeling violated by the disclosure of my personal information, I also feel scared. As described above, I question how secure my information is. I do not know who can access my data, and I fear that my information may be weaponized against me for political retribution or other improper purposes.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 17, 2026, in Texas.



Haley Smith

Exhibit K

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

vs.

Case No. 1:26-cv-01352-SLS

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

DECLARATION OF ALEX DOE

I, Alex Doe, declare as follows:

1. I am over 18 years old and a member of Common Cause of Texas. The statements made in this declaration are based on my personal knowledge, information, and belief. I submit this declaration in support of Plaintiffs' motion for summary judgment.

2. I have been a United States citizen for over a decade.

3. I was born in South America. I immigrated to the United States with my parents when I was a toddler.

4. I was issued a Social Security Number (SSN) and card in the early 2010s, when I was in elementary school. At the time I applied for an SSN, I was a lawful permanent resident.

5. My parents became naturalized U.S. citizens in the 2010s. I automatically became a U.S. citizen when my father naturalized.

6. I was issued a U.S. passport, confirming my U.S. citizenship. It was most recently updated in the last five years.

7. When my parents became U.S. citizens, they instilled in me the power and importance of voting. Ever since, I have taken my responsibility to vote seriously. I consider it to

be one of the primary ways we as Americans can express ourselves, our needs, and our desires in order to inform the government and improve our communities. I understand that to vote is to have a voice in society.

8. After turning 18, I registered to vote, and I regularly vote in state and federal elections in Texas. I'm proud that I have voted in nearly every election in the past six years.

9. I currently live in and am registered to vote in Texas. In order to register to vote in Texas, I provided my name; date of birth; residential address; driver's license number or last four digits of my SSN; and telephone number. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.

10. I recently voted on the first day of early voting in Texas' primary election, and I intend to vote in the November midterm elections in Texas this year.

Department of Homeland Security's Expanded SAVE System Led to the Cancellation of My Voter Registration and Other Burdens on My Voting Rights

11. Last October, I received a letter from my County Elections Administrator/Voter Registrar, titled "Notice to Registered Voter for Proof of Citizenship (USCIS Verification)." A true and correct copy of the letter, with certain private information redacted, is attached hereto as Exhibit 1.

12. I did not open the letter for a while. I am busy working toward a postgraduate degree and the envelope looked like it was unofficial. The envelope did not indicate that it was official election mail, that it was urgent, or that any action was required from me to stay registered to vote. It looked like junk mail, or even a scam.

13. I eventually opened the letter. It said that the government did not think I was a U.S. citizen, and that I would be dropped from the voting rolls unless I provided proof of my U.S. citizenship by emailing a photo of my passport to a email address purportedly belonging to

the County Elections Department. At that point, I only had a week until the deadline.

14. Because the process seemed so informal, I was still skeptical that this was an official government process. I even emailed the County Elections Department to confirm that sending a picture of my passport to a random email address was the expectation. Ultimately, I did email a scan of my passport to the County Elections Office in order to preserve my right to vote.

The Department of Justice Is Collecting, Disclosing, and Repurposing My Personal Data Without My Consent, Causing Me Distress and Risking Burdening My Fundamental Right to Vote

15. I later learned more about DHS’s SAVE system and the Department of Justice (“DOJ”) efforts to compile every state’s and Washington D.C.’s voter rolls in service of creating a nationwide voter roll list and using states’ voter tolls to conduct voter roll list maintenance.

16. I learned that, in 2025, DHS expanded the SAVE system by allowing bulk searches of Americans’ personal data housed at the Social Security Administration (“SSA”), using only a name, date of birth, and SSN.¹ I also learned that the Texas Secretary of State had announced in a press release on October 20, 2025, that her office had used this new functionality to run Texas’s entire voter registration list with more than 18 million voters through the expanded SAVE system, that they identified “2,724 potential noncitizens” who were registered to vote in Texas, and that they referred those individuals to Texas counties to determine their eligibility to vote.² The Secretary further stated that once the counties complete this process, “individuals who are deemed noncitizens that voted in a Texas election will be referred to the Office of the Attorney General” for investigation.

1

<https://www.uscis.gov/save/current-user-agencies/guidance/voter-registration-and-voter-list-maintenance-fact-sheet>;

<https://www.federalregister.gov/documents/2025/10/31/2025-19735/privacy-act-of-1974-system-of-records>.

² <https://www.sos.state.tx.us/about/newsreleases/2025/102025.shtml>.

17. Based on the Texas Secretary of State's October 20 press release and the October 21 letter I received, it is my understanding that I am one of the "2,724 potential noncitizens" identified through DHS's expanded SAVE system.

18. It is my understanding that, as part of the process of bulk uploading Texas's entire voter registration list into SAVE, the Texas Secretary of State disclosed, at a minimum, my name, date of birth, and either my driver's license number or last four digits of my SSN to DHS, and that this information will be retained in SAVE for at least 10 years. It is my understanding that after the Texas Secretary of State uploaded my voter registration information into DHS's SAVE system, DHS disclosed that information to SSA so that SSA could match it against its own records about me.

19. It is my understanding that the Texas Secretary of State, after executing a Memorandum of Understanding with DOJ similarly provided DOJ with Texas's entire voter registration list as part of the DOJ's efforts to compile voter data from all 50 states and the District of Columbia. It is my understanding that the voter list Texas sent to DOJ included information such as my name, date of birth, address, and driver's license number or last four digits of my SSN.

20. I have not consented to, and do not consent to, the Texas Secretary of State disclosing the information about me that her office shared with DOJ. I provided that information for use by state and local Texas officials, not to be uploaded into a national voter database at DOJ or national citizenship database housed at DHS. I expected that information—especially my driver's license number and SSN—to remain private and protected by state and local Texas officials.

21. It is my understanding that DOJ intends to disclose the voter registration lists it

collects from the states—including Texas—to DHS so that it can run the data through the SAVE system. It is my understanding that the DOJ MOU requires Texas to remove any voters DOJ identifies as ineligible to vote from Texas’s voter roll. I also have not consented to, and do not consent to, DOJ disclosing that information with DHS through the SAVE system.

22. It is also my understanding that the DOJ MOU allows the DOJ to disclose personally identifiable information (“PII”) to private contractors to assist with list maintenance verification. It is not clear to me what “list maintenance verification procedures” are, or who these contractors might be. I never consented to, nor do I consent to, DOJ sharing my personal information with anyone outside of the government.

23. I am disturbed, uneasy, anxious, and frustrated that the government has violated my trust by collecting, disclosing, matching, and repurposing my personal information without my consent in an effort to create a national database of voters. I am also worried that DOJ may be seeking to create a new, comprehensive list of voters who were born abroad in order to target, surveil, or simply make life harder for foreign-born American citizens. This makes me feel like I am living in a surveillance state where government actors can access my most private information at will. I expected the United States to respect all of its citizens’ privacy, but instead I am opposing government efforts to create a centralized profile on me, including my sensitive information, for a national voter database.

24. I am also concerned that by collecting voter data from many different states, DOJ is incentivizing hackers or bad actors to try to gain access to data that is otherwise maintained in a decentralized manner by each individual state. My concerns are amplified by my knowledge of the current administration’s history of misusing and failing to protect personal data.

25. Because DOJ intends to share my sensitive personal information across federal

agencies and with private contractors, I am also deeply worried that my data will be stored or transferred in an unsecured manner, exposing me to a data breach and identity theft and fraud. I am especially concerned about the unsecured storage or transfer of files containing information such as my full name, date of birth, address, and driver's license number or last four digits of my SSN, because the exposure of those data elements in tandem creates a heightened risk of identity theft and fraud. This fear is especially heightened by the DOJ's purported authority to share such sensitive personal information with third-party contractors outside of the government, as outlined in its MOU with Texas.

26. I deeply value and cherish my right to vote. I am greatly concerned that I will be purged from the voter rolls again based on Texas sharing my voter data with DOJ and the statements in the DOJ MOU suggesting Texas is required to "clean" its voter rolls based on DOJ identifying purported voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns. I am also greatly concerned that I will be wrongly investigated by DOJ or other federal agencies based on DOJ's review of Texas's voter rolls.

27. I am particularly worried because DOJ intends to rely on or is already relying on SAVE and SSA citizenship data, which I have personally confirmed is inaccurate and out of date for me.

28. Texas has already incorrectly misidentified me as a noncitizens once using that inaccurate information. It is my understanding that DOJ is referring the purported noncitizen voters it identifies to Homeland Security Investigations, and I am extremely worried about being wrongly investigated because of DOJ relying on inaccurate information that wrongly suggests I am a noncitizen voter.

29. When Texas wrongly misidentified me as a noncitizen because of the State's use

of SAVE, I was so confused that I tried calling the SSA to see what information they had on me. I was surprised to learn that the agency did not have information on my citizenship status one way or the other, even though they should--they told me that my citizenship status in their records was "unknown." This made me even more confused and anxious. With everything going on, sometimes I fear DHS may even show up at my door, even though I am a U.S. citizen, because they are relying on inaccurate and incomplete information about me.

30. Being wrongly misidentified as a noncitizen and threatened with removal from the voter rolls caused a mix of emotions. The government questioning my citizenship, my right to be here, and my right to vote made me feel like they were questioning my entire identity. I was surprised, confused, upset, and offended that I had to confirm my citizenship. I'm here legally; I've voted in every election since I was 18; I've never been in trouble with the law. I didn't—and still don't—understand why my vote came into question.

31. I was also a little bit disturbed. Prior to this experience, I had certain expectations that the government was functional and organized. I always assumed that the government had correct information about me and that it was taking measures to keep my data secure. Learning firsthand that the government's information about me is so disorganized and inaccurate, and that they are using my information so haphazardly, has been disappointing and made me lose a little bit of faith in our institutions.

32. The process of sending in my passport photo also made me feel anxious. My partner works in cybersecurity, and I understand that emailing sensitive documents as attachments is not typically considered to be safe. If the government needed me to submit such sensitive documents, I would have expected that it would take steps to protect my information and ensure enhanced security, like requiring that I upload the passport to a secure portal.

33. The inaccuracy of the data made me worried that Texas will continue to wrongly identify me as ineligible to vote. As a result, even though I have voted many times before, I was nervous about voting in the most recent primary election in a way that I have not been before. Even though I had confirmed my voter registration when I submitted my passport at the end of last year, I still re-checked my voter registration the week before voting because I was paranoid that the government may have messed up my information and gone through with their threat to purge me from the voter rolls. For the first time, I brought my passport when I went to vote just in case my citizenship or eligibility was questioned. Throughout the process of voting, paranoia about my ability to vote was in the back of my mind.

34. These fears were only heightened when I learned that the Texas Secretary of State recently executed the DOJ MOU to share Texas's voter registration data with DOJ and to surrender its voter list maintenance responsibilities to the federal government.

35. I am also worried that, even though I recently provided my county with documentary proof of citizenship and my voter registration was reinstated, DOJ will continue to wrongly identify me as a non-citizen based on faulty underlying data when DOJ runs bulk voter roll searches in the future, and that I will again be forced to prove my citizenship status in order to retain my voter registration. Being caught in such a cycle, with my voting rights on the line, is distressing to me.

36. I fear that I will be forced to prove my citizenship status again and am distressed that I have to remain vigilant about my voter registration status. I plan to continue voting regularly, and now feel compelled to regularly check my voter registration status to ensure that it is not wrongly cancelled.

37. The privacy of my personal information—including the data contained in my

voter file—is very important to me. From a young age, my parents instilled in me the importance of protecting the confidentiality of my personal information such as my SSN and driver’s license number, and so I have always treated my Social Security card and driver’s license as ultra sensitive documents. Moreover, because I pay taxes and plan to retire and receive Social Security benefits in the future, SSA has personal information about me that I consider highly sensitive. I have trusted SSA and Texas election officials to keep my information private and only use it for lawful purposes. I understood them to be bound by laws that would keep them from sharing this information across government agencies for completely unrelated purposes. I did not consent to them sharing this highly sensitive information with the federal government for unlawful or undisclosed purposes.

38. It is extremely concerning that so many people across all levels of government have access to my personal data without my consent. I am skeptical of any unauthorized national database, but especially one that contains my private data and lets government officials access and utilize it in a way that can be used against me and others similarly situated.

39. Beyond feeling violated by the disclosure of my personal information, I also feel scared. As described above, I question how secure my information is. I do not know who can access my data, and I fear that my information may be weaponized against me for political retribution or other improper purposes.

40. I am submitting this declaration under a pseudonym to protect myself and my school from possible retaliation. This administration (and state leaders in Texas) is vindictive about going after perceived political enemies, and I worry that I could be a target by participating in a lawsuit that threatens their voter purge efforts. The Trump administration has threatened to try and denaturalize people who oppose the administration’s policies, and has targeted

universities for taking actions the administration doesn't agree with. I fear that the Trump administration could take similar steps towards me or my university if it knows my identity.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 15, 2026, in Texas.

A handwritten signature in blue ink that reads "A. Doe". The signature is written in a cursive, slightly stylized font.

Alex Doe*

* Out of fear of retaliation and harassment, Alex Doe submits this declaration under pseudonym. Counsel for Plaintiffs hereby certify that they have an unaltered signed copy of the foregoing document available for inspection by the Court

EXHIBIT 1

21-50
Prescribed by Secretary of State
Section 16.033, Texas Election Code
10/2025

ELECTIONS ADMINISTRATION

NOTICE TO REGISTERED VOTER FOR PROOF OF CITIZENSHIP (USCIS VERIFICATION)

Dear [REDACTED]

As the voter registrar for [REDACTED] I am writing to notify you of important information regarding your voter registration.

You are currently registered to vote in this county. We have received information from the Texas Secretary of State reflecting that you might not be a United States citizen. A comparison of the information in your voter registration records with the United States Citizenship and Immigration Services SAVE records show that you were not a United States citizen at the time of the comparative process. Although you can obtain United States and state government identity documents as a non-United States citizen, only United States citizens are eligible to vote.

To maintain your active voter registration status, please provide proof that you are a United States citizen. Proof of United States citizenship can be established by presenting a copy of any of the following documents:

- U.S. birth certificate or a Consular Report of Birth Abroad of a Citizen of the United States issued by the United States Department of State;
- United States passport;
- Certificate of Naturalization or Certificate of Citizenship; or
- Your parent's Certificate of Naturalization along with your birth certificate if you became a U.S. citizen as a result of your parent's naturalization.

There are several ways to provide proof of U.S. citizenship to my office. You can deliver it by hand, or you can send it by mail, fax, electronic mail, or any other method of transmission. My office's contact information is listed at the top of this letter.

Please provide proof of U.S. citizenship within thirty (30) days from the date of this letter. If we do not receive a response from you within thirty (30) days, your voter registration will be cancelled. In the event that your registration is cancelled, you can still be immediately reinstated by providing proof of U.S. citizenship to my office or at your polling location, even if the thirty (30)-day period has already passed. You may also request a hearing to challenge your cancellation, even if you do not possess one of the above forms, by contacting my office.

If you have any questions regarding this notice or your voter registration, please contact my office at [REDACTED]

10 [REDACTED] 2025
Date

Exhibit L

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

vs.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF BAILEY DOE

I, Bailey Doe, declare as follows:

1. I am over 18 years old and a member of Common Cause of Texas. The statements made in this declaration are based on my personal knowledge, information, and belief. I submit this declaration in support of Plaintiffs' motion for summary judgment.

Background

2. I have been a United States citizen since 2021.
3. I was born in Mexico in 1996. I immigrated to the United States with my family when I was a baby.
4. I was issued a Social Security Number ("SSN") and card in 2015, when I was nineteen years old. When I applied for an SSN, I was a lawful permanent resident.
5. I was naturalized in 2021, when I was twenty-five years old.
6. I have a Certificate of Naturalization, issued in September 2021.
7. I was issued a U.S. passport, confirming my U.S. citizenship, in November 2021.

8. After becoming a U.S. citizen, I knew I now had the right to vote in U.S. elections. I felt excited to participate as a way to make my voice heard on the issues that matter to me. I felt that it was important to vote because it is a fundamental right of U.S. citizenship.

9. I registered to vote in 2024 and began voting in state and federal elections in Texas. In order to register to vote in Texas, I provided my name; date of birth; residential address; driver's license number or last four digits of my SSN; and telephone number. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.

10. I currently live in and, until recently, was registered to vote in Texas. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.

DHS's Expanded SAVE System Led to the Cancellation of My Voter Registration and Other Burdens on My Voting Rights

11. After voting in the November 2025 election, I received a letter from my county elections office, dated mid December 2025, titled "Notice of Cancellation of Voter Registration." A true and correct copy of the letter, with certain identifying information redacted, is attached as Exhibit 1 ("the Cancellation Notice").

12. The exterior of the envelope in which the letter was enclosed had no markings indicating it was official election mail or that the enclosed letter had any bearing on my voter registration.

13. The Cancellation Notice states that "[n]otice is hereby given that your voter registration has been cancelled in [*redacted to preserve pseudonymity*] County. The reason for cancellation was: The reason for cancellation is due to failure to respond to a Notice of Examination mailed to you by this office over 30 days ago. (Sec. 16.033, Texas Code)."

14. I never received the referenced "Notice of Examination" that my county elections office claimed to have sent to me.

15. The Cancellation Notice further states that “[y]ou may request a hearing on the cancellation of your registration by submitting a written request for such hearing. If you request a hearing, a notice will be mailed to you setting forth the date of the hearing. The hearing will be scheduled within ten (10) days after your request or on a later date if you so request. If after the hearing, the voter registrar determines that your registration shall remain cancelled, you are entitled to appeal the adverse decision issued by the voter registrar by petitioning for review in district court not later than the 30th day after the adverse decision is issued.”

16. From the text of the Cancellation Notice, I could not determine why I had been issued a “Notice of Examination” or why my voter registration was being called into question in the first place.

17. In the weeks after receiving the Cancellation Notice, I searched for my name in my county’s Voter Lookup Tool, and my registration was no longer active.

18. I was initially scared to even call or go visit my county elections office because I know that federal immigration officers, including ICE, have been showing up at courthouses and other government buildings to question and arrest people.

19. In February 2026, I called my county elections office to ask for a copy of the Notice of Examination that was supposedly sent to me, but that I never received in the mail, and for information on why my voter registration had been cancelled. My county elections office refused to provide me with a copy of the Notice of Examination unless I submitted a written public records request asking for the Notice. So I submitted a records request at the end of February in advance of the March 3 elections.

20. A few days later, while I was waiting for my records request to be answered, I made two follow-up calls to my county elections office to ask them to tell me why my voter registration had been cancelled and how I could fix this.

21. In the second phone call, the employee I spoke to confirmed that my voter registration was cancelled because I failed to respond to a prior Notice of Examination. The employee did not tell me that I had been removed due to suspected non-citizenship. The employee said that the county elections office had a record of sending the Cancellation Notice, which I had received, but that the office did not have a record of sending any Notice of Examination to me.

22. In the third phone call, the employee I spoke to informed me that my name had appeared on a list of suspected noncitizens that the county elections office had received from the Texas Secretary of State's office back in October 2025 after the Secretary had used DHS's SAVE system to review the state's voter rolls. The employee said that my inclusion on that list was the basis for sending the Notice of Examination to me. The employee said that they did not have a scanned copy of the Notice of Examination that the office supposedly sent to me because the county only saves scans of notices if they mail them to a second address. Because they had no scanned copy of a mailed Notice of Examination on file for me, the employee said their response to my records request would likely just be a generic copy of the Notice of Examination. The employee told me the date their records indicate that the Notice of Examination was supposedly sent to me, but the date they provided made no sense to me as it was the same December 2025 date that is on the Cancellation Notice I received.

23. In at least two separate phone calls with my county elections office, I was told that, in order to have my voter registration reactivated and be able to vote again, I would need to

submit a new voter registration application and attach a copy of documentary proof of citizenship (“DPOC”). These instructions were different from what I had seen in public materials, including a press release from the Texas Secretary of State, which conveyed that Texas voters who had been cancelled for suspected non-citizenship would be reinstated immediately if they showed DPOC.¹ When I asked the employee about this, the employee maintained that submitting a new application was the only way to get back on the voter rolls.

24. After the March 3, 2026, elections, my county elections office responded to my records request and produced to me a document titled “Notice to Registered Voter for Proof of Citizenship (USCIS Verification)” (“Notice of Examination”). The Notice of Examination identifies me by name but is dated March 6, 2026, which shows that this is just a generic copy of the Notice of Examination and not a scan of any notice that was mailed to me. A true and correct copy of the Notice of Examination, with certain identifying information redacted, is attached as Exhibit 2.

25. The Notice of Examination states in part that a “comparison of the information in your voter registration records with the United States Citizenship and Immigration Services SAVE records show that you were not a United States citizen at the time of the comparative process.” It then instructs: “[t]o maintain your active voter registration status, please provide proof that you are a United States citizen.” The Notice of Examination lists several types of documents that will be accepted as proof of U.S. citizenship, and notes that copies of the documents can be delivered by hand, mail, fax, email, or any other method of transmission.

26. The Notice of Examination confirms what an employee at my county elections office told me in a phone call: my name had appeared on a list of suspected noncitizens that the

¹ <https://www.sos.state.tx.us/about/newsreleases/2025/102025.shtml>.

county elections office had received from the Texas Secretary of State's office back in October 2025 after the Secretary had used DHS's SAVE system to review the state's voter rolls.

27. The Notice of Examination further states: "Please provide proof of U.S. citizenship within (30) days from the date of this letter. If we do not receive a response from you within thirty (30) days, your voter registration will be cancelled."

28. When the employee at the county elections office told me I was on a list of suspected noncitizens that was created by Texas election officials searching DHS's SAVE system and again when I received the Notice of Examination in response to my records request, I was shocked. As stated above, I have been a citizen with a U.S. passport since 2021. I was worried that the letter was part of a voter suppression effort to discourage Texans from exercising their right to vote, which I found alarming and troubling as someone who strongly believes in the right to vote.

29. The experience has also made me feel demotivated and disillusioned, as it has been very challenging to get clear information or guidance from my county elections office. It took three phone calls to confirm that my registration had been cancelled for suspected noncitizenship. In multiple phone calls with my county elections office, I was never told that my registration could be reinstated immediately upon providing DPOC to either my county elections office or at the polls and that I would be able to vote in the March 3 elections if I did so. Instead, I was instructed to submit a new voter registration application, which was different from what I had seen in public materials. The confusion left me feeling afraid to do the wrong thing and potentially get in trouble or be subject to more investigations.

30. As of the date of this declaration, based on what I have seen in my county's voter registration look-up, it is my understanding that my voter registration remains cancelled.

31. My voter registration remained cancelled during the voting period for the March 3, 2026, primary election in Texas, and I was unable to vote. If I am able to get my voter registration reinstated, I intend to vote in the November 2026 midterm elections in Texas.

The Department of Justice Is Collecting, Disclosing, and Repurposing My Personal Data Without My Consent, Causing Me Distress and Risking Burdening My Fundamental Right to Vote

32. After my voter registration was cancelled, I learned more about DHS's SAVE system and the Department of Justice ("DOJ") efforts to compile every state's and Washington D.C.'s voter rolls in service of creating a nationwide voter roll list and using states' voter rolls to conduct voter roll list maintenance

33. I learned that, in 2025, DHS expanded the SAVE system by allowing bulk searches of Americans' personal data housed at the Social Security Administration ("SSA"), using only a name, date of birth, and either my driver's license number or last four digits of my SSN.² I also learned that the Texas Secretary of State had announced in a press release on October 20, 2025, that her office had used this new functionality to run Texas's entire voter registration list with more than 18 million voters through the expanded SAVE system, that they identified "2,724 potential noncitizens" who were registered to vote in Texas, and that they referred those individuals to Texas counties (including my county) to determine their eligibility to vote.³ The Secretary further stated that once the counties complete this process, "individuals who are deemed noncitizens that voted in a Texas election will be referred to the Office of the Attorney General" for investigation.

²

<https://www.uscis.gov/save/current-user-agencies/guidance/voter-registration-and-voter-list-maintenance-fact-sheet>;
<https://www.federalregister.gov/documents/2025/10/31/2025-19735/privacy-act-of-1974-system-of-records>.

³ <https://www.sos.state.tx.us/about/newsreleases/2025/102025.shtml>.

34. Based on the Texas Secretary of State's October 20 press release, the information provided to me by the employee I spoke with at my county elections office, and the Notice of Examination provided to me in response to my records request, it is my understanding that I am one of the "2,724 potential noncitizens" identified through DHS's expanded SAVE system.

35. It is my understanding that, as part of the process of bulk uploading Texas's entire voter registration list into SAVE, the Texas Secretary of State disclosed, at a minimum, my name, date of birth, and driver's license number or last four digits of my SSN to DHS, and that this information will be retained in SAVE for at least 10 years. It is my understanding that after the Texas Secretary of State uploaded my voter registration information into DHS's SAVE system, DHS disclosed that information to SSA so that SSA could match it against its own records about me.

36. It is my understanding that the Texas Secretary of State, after executing a Memorandum of Understanding with DOJ similarly provided DOJ with Texas's entire voter registration list as part of the DOJ's efforts to compile voter data from all 50 states and the District of Columbia. It is my understanding that the voter list Texas sent to DOJ included information such as my name, date of birth, address, and driver's license number or last four digits of my SSN.

37. It is my understanding that DOJ intends to disclose the voter registration lists it collects from the states—including Texas—to DHS so that it can run the data through the SAVE system. It is my understanding that the DOJ MOU requires Texas to remove any voters DOJ identifies as ineligible to vote from Texas's voter roll.

38. It is also my understanding that the DOJ MOU allows the DOJ to disclose personally identifiable information (“PII”) to private contractors to assist with list maintenance verification.

39. I have not consented to, and do not consent to, the Texas Secretary of State disclosing the information about me that her office shared with DOJ. I provided that information for use by state and local Texas officials, not to be uploaded into a national voter database at DOJ or national citizenship database housed at DHS. I expected that information—especially my driver’s license number and SSN—to remain private and protected by state and local Texas officials.

40. I also have not consented to, and do not consent to, DOJ disclosing that information with DHS through the SAVE system or with private contractors.

41. I am disturbed, uneasy, anxious, and saddened that the government has violated my trust by collecting, disclosing, matching, and repurposing my personal information without my consent in an effort to create a national database of voters. I am also worried that DOJ may be seeking to create a new, comprehensive list of voters who were born abroad in order to target, surveil, or simply make life harder for foreign-born American citizens. I no longer feel like my U.S. passport and U.S. citizenship will protect me from intrusive investigations by the government if I can be accused of being a noncitizen at any time. I expected the United States to respect all of its citizens’ privacy, but instead I am opposing government efforts to create a centralized profile on me, including my sensitive information, for a national voter database.

42. I am also concerned that by collecting voter data from many different states, DOJ is incentivizing hackers or bad actors to try to gain access to data that is otherwise maintained in

a decentralized manner by each individual state. My concerns are amplified by my knowledge of the current administration's history of misusing and failing to protect personal data.

43. Because DOJ intends to share my sensitive personal information across federal agencies and with private contractors, I am also deeply worried that my data will be stored or transferred in an unsecured manner, exposing me to a data breach and identity theft and fraud. I am especially concerned about the unsecured storage or transfer of information such as my full name, date of birth, address, and driver's license number or last four digits of SSN, because the exposure of those data elements in tandem creates a heightened risk of identity theft and fraud. This fear is especially heightened by the DOJ's purported authority to share such sensitive personal information with third-party contractors outside of the government, as outlined in its MOU with Texas.

44. I deeply value and cherish my right to vote. I am greatly concerned that I will be purged from the voter rolls again based on Texas sharing my voter data with DOJ and the statements in the DOJ MOU suggesting Texas is required to "clean" its voter rolls based on DOJ identifying purported voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns. I am also greatly concerned that I will be wrongly investigated by DOJ or other federal agencies based on DOJ's review of Texas's voter rolls.

45. I am particularly worried because DOJ intends to rely on or is already relying on SAVE and SSA citizenship data, which I have personally confirmed is inaccurate and out of date for me.

46. Texas has already incorrectly removed me from the voter rolls once using that inaccurate information. It is my understanding that DOJ is referring the purported noncitizen voters it identifies to Homeland Security Investigations, and I am extremely worried about being

wrongly investigated because of DOJ relying on inaccurate information that wrongly suggests I am a noncitizen voter.

47. I had to make multiple phone calls in February and March 2026 before I was able to speak to a human at SSA. The SSA employee I spoke with on the phone told me that I am (incorrectly) listed as a non-citizen in SSA's records. That was not surprising to me, because the only prior time I had interacted with SSA was when I obtained a Social Security card in 2015, before I became a U.S. citizen. To my knowledge, there is no requirement for me to update my citizenship status with SSA, and I have not done so.

48. As long as Texas and DOJ intend to use the expanded SAVE system and the unreliable data it utilizes, I will feel compelled to continue regularly checking my voter registration status to ensure it is not wrongly cancelled again.

49. It is my understanding that, based on the previous SAVE search of my personal information, SSA has already returned a response to DHS that included my SSN, name, date of birth, an indicator of my citizenship status, and other information that SSA collected when I applied for a Social Security card in 2015. It is my understanding that my personal SSA data will be retained in DHS's SAVE system for at least 10 years.

50. I have not consented to, and do not consent to, SSA disclosing and verifying my personal information from SSA records to DOJ, DHS, or any other federal, state, or local agency to run citizenship checks for voter list maintenance or any other purpose. I expected that data to remain private within SSA and be used only for purposes consistent with why SSA collected the data, such as to determine eligibility for SSA benefits or authorization to work in the U.S. I never expected my personal SSA information to be disclosed to DOJ, DHS, or any other federal, state, or local agency for use in a massive national citizenship database for voter eligibility checks.

51. I am distressed and saddened by the fact that the government has repurposed my sensitive SSA data without my consent to determine my eligibility to vote, when the information is not suitable for that purpose and was never intended to be used in that way. It was a significant moment in my life when I received my SSN because having an SSN allowed me to go to college and get a job. Learning that my SSA data has been shared without my consent is distressing because it makes me feel vulnerable and nervous like I felt before I became a U.S. citizen.

52. I am also worried that, even if I provide my county elections office with documentary proof of citizenship and my voter registration is reinstated, DHS's SAVE system will continue to wrongly identify me as a non-citizen based on faulty underlying data when DOJ runs bulk voter roll searches in the future, and that I will again be forced to prove my citizenship status in order to retain my voter registration. Being caught in such a cycle, with my voting rights on the line, is distressing to me. I now worry that the federal government can simply say whenever it wants that I am no longer a citizen.

53. The privacy of my personal information—including the data contained in my voter file—is very important to me. Receiving my Social Security card was an important moment in my life that allowed me to go to college and get a job. I treat my Social Security card and driver's license as ultra sensitive documents and closely guard my personal information. Moreover, because I pay taxes and plan to retire and receive Social Security benefits in the future, SSA has personal information about me that I consider highly sensitive. I have trusted SSA and Texas election officials to keep my information private and only use it for lawful purposes. I understood them to be bound by laws that would keep them from sharing this information across government agencies for completely unrelated purposes. I did not consent to them sharing this highly sensitive information with the federal government for unlawful or

undisclosed purposes.

54. It is extremely concerning that so many people across all levels of government have access to my personal data without my consent. I am skeptical of any unauthorized national database, but especially one that contains my private data and lets government officials access and utilize it in a way that can be used against me and others similarly situated.

55. Beyond feeling violated by the disclosure of my personal information, I also feel scared. As described above, I question how secure my information is. I do not know who can access my data, and I fear that my information may be weaponized against me for political retribution or other improper purposes.

56. I am requesting to file this declaration under a pseudonym because I fear retaliation from the current administration for speaking up. Given the countless actions this administration has taken against individuals who oppose it, I fear that the government will retaliate against me. I have concerns that my status as a naturalized citizen will be used against me unless I can submit this declaration under a pseudonym.

57. I fear, given the memo published by DOJ indicating they are going to pursue denaturalizing citizens as a punishment, that if I were to identify myself as a naturalized citizen publicly opposing the administration's policies then the administration would take retaliatory action against me or my naturalized family members, including investigating us to seek denaturalization. Finally, I have family members (who are also naturalized) currently living in a state that, by my understanding, is complying with DOJ's efforts to purge voter rolls and open criminal investigations.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 15, 2026, in Texas.

Bailey Doe

Bailey Doe*

*Out of fear of retaliation and harassment, Bailey Doe submits this declaration under pseudonym. Counsel hereby certifies that they have an unaltered signed copy of the foregoing document available for inspection by the Court.

Exhibit 1

[Redacted]
Elections Administrator

[Redacted]
Assistant Elections Administrator

12/ [Redacted] 2025

Id number: [Redacted]

Prescribed by Secretary of State Sections 16.031(a), 16.036, Texas Election Code 9/2023

NOTICE OF CANCELLATION OF VOTER REGISTRATION

Notice is hereby given that your voter registration has been cancelled in [Redacted] County.
The reason for cancellation was:

The reason for cancellation is due to failure to respond to a Notice of Examination mailed to you by this office over 30 days ago. (Sec. 16.033, Texas Code).

You may request a hearing on the cancellation of your registration by submitting a written request for such hearing. If you request a hearing, a notice will be mailed to you setting forth the date of the hearing. The hearing will be scheduled within ten (10) days after your request or on a later date if you so request.

If after the hearing, the voter registrar determines that your registration shall remain cancelled, you are entitled to appeal the adverse decision issued by the voter registrar by petitioning for review in district court not later than the 30th day after the adverse decision is issued.

If you should have any questions regarding this cancellation, please contact me at [Redacted]

[Redacted]
Voter Registration Clerk

[Redacted]

Exhibit 2

[REDACTED]
Elections Administrator

[REDACTED]
Assistant Elections Administrator

03/06/2026

Id number: [REDACTED]

21-50 Prescribed by Secretary of State Section 16.033, Texas Election Code 10/2025

NOTICE TO REGISTERED VOTER FOR PROOF OF CITIZENSHIP (USCIS VERIFICATION)

Dear Voter: [REDACTED]

As the voter registrar for [REDACTED] County, I am writing to notify you of important information regarding your voter registration.

You are currently registered to vote in this county. We have received information from the Texas Secretary of State reflecting that you might not be a United States citizen. A comparison of the information in your voter registration records with the United States Citizenship and Immigration Services SAVE records show that you were not a United States citizen at the time of the comparative process. Although you can obtain United States and state government identity documents as a non-United States citizen, only United States citizens are eligible to vote.

To maintain your active voter registration status, please provide proof that you are a United States citizen. Proof of United States citizenship can be established by presenting a copy of any of the following documents:

- U.S. birth certificate or a Consular Report of Birth Abroad of a Citizen of the United States issued by the United States Department of State;
- United States passport;
- Certificate of Naturalization or Certificate of Citizenship; or
- Your parent's Certificate of Naturalization along with your birth certificate if you became a U.S. citizen as a result of your parent's naturalization.

There are several ways to provide proof of U.S. citizenship to my office. You can deliver it by hand, or you can send it by mail, fax, electronic mail, or any other method of transmission. My office's contact information is listed at the bottom of this letter.

Please provide proof of U.S. citizenship within thirty (30) days from the date of this letter. If we do not receive a response from you within thirty (30) days, your voter registration will be cancelled. In the event that your registration is cancelled, you can still be immediately reinstated by providing proof of U.S. citizenship to my office or at your polling location, even if the thirty (30)-day period has already passed. You may also request a hearing to challenge your cancellation, even if you do not possess one of the above forms, by contacting my office.

If you have any questions regarding this notice or your voter registration, please contact my office at [REDACTED]

[REDACTED]
Elections Administrator

[REDACTED]

Id number: [REDACTED]

21-50 Prescribed by Secretary of State Section 16.033, Texas Election Code 10/2025

AVISO AL VOTANTE REGISTRADO PARA PRESENTAR PRUEBA DE SU CIUDADANÍA (VERIFICACIÓN DE USCIS)

Estimado votante, [REDACTED]

Como el Registrador de Votantes del Condado de [REDACTED] me comunico con usted para hacerle llegar información importante con respecto a su registro electoral.

Usted está actualmente registrado para votar en este condado. Hemos recibido información de la Secretaría de Estado de Texas que refleja que usted podría no ser un ciudadano de los Estados Unidos. Una comparación entre la información de su registro de votante y los registros del Sistema SAVE del Servicio de Ciudadanía e Inmigración de los Estados Unidos (USCIS) indica que usted no era ciudadano estadounidense en el momento del proceso comparativo. Aunque puede obtener documentos de identidad del gobierno de los Estados Unidos y del estado como ciudadano no estadounidense, solo los ciudadanos estadounidenses tienen derecho a votar.

Para mantener su estado de votante registrado activo, le solicitamos que nos proporcione prueba de que usted es un ciudadano de los Estados Unidos. La prueba de la ciudadanía de los Estados Unidos se puede establecer presentando una copia de cualquiera de los siguientes documentos:

- Certificado de nacimiento estadounidense o Certificado consular de nacimiento en el extranjero emitido por el Departamento de Estado de los Estados Unidos;
- Pasaporte estadounidense;
- Certificado de naturalización o Certificado de ciudadanía; o
- Certificado de naturalización de su padre o madre junto con su Certificado de nacimiento, si se convirtió en ciudadano estadounidense como resultado de la naturalización de su padre o madre.

Hay varias maneras de proporcionar la prueba de su ciudadanía estadounidense a mi oficina. Puede traerla personalmente, enviarla por correo, fax, correo electrónico o por cualquier otro método de transmisión. La información de contacto de mi oficina se detalla al pie de esta carta.

Favor proporcionar la prueba de su ciudadanía estadounidense dentro de los treinta (30) días a partir de la fecha de esta carta. Si no recibimos una respuesta dentro de los próximos treinta (30) días, su registro electoral será cancelado. Si su registro electoral se cancela, puede reinscribirse inmediatamente al presentar la prueba de su ciudadanía estadounidense en mi oficina o en el lugar de votación que le corresponde, aún después del plazo de treinta (30) días. También puede solicitar una audiencia para impugnar la cancelación, incluso si no posee uno de los documentos anteriores, comunicándose con mi oficina.

Si tiene alguna pregunta con respecto a este aviso o sobre su registro electoral, comuníquese con mi oficina al [REDACTED]

[REDACTED]
Administrador de Elecciones

THÔNG BÁO ĐẾN CỬ TRI ĐÃ GHI DANH VỀ CHỨNG MINH CÔNG DÂN (USCIS XÁC MINH)

Kính Gửi Cử Tri: [REDACTED]

Là người đăng ký cử tri cho Quận [REDACTED] Tôi viết thư để thông báo cho quý vị về thông tin quan trọng liên quan đến việc đăng ký cử tri của quý vị. Quý vị hiện được đăng ký bỏ phiếu tại quận này. Chúng tôi đã nhận được thông tin từ Tổng Thư Ký Tiểu Bang Texas phản ánh rằng quý vị có thể không phải là công dân Hoa Kỳ. Một so sánh thông tin hồ sơ ghi danh cử tri của quý vị với hồ sơ công dân Hoa Kỳ và số Di Trú Hệ Thống Kiểm Tra Tình Trạng Hồ Sơ Di Trú cho thấy quý vị không phải là công dân Hoa Kỳ lúc kiểm tra so sánh tiến hành. Cho dù quý vị có được vào Hoa Kỳ và có giấy tờ nhận dạng của chính quyền tiểu bang xác định là người không phải công dân Hoa Kỳ, chỉ có công dân Hoa Kỳ mới có đủ điều kiện để bỏ phiếu.

Để duy trì tình trạng đăng ký cử tri có hiệu lực của quý vị, vui lòng cung cấp bằng chứng rằng quý vị là công dân Hoa Kỳ. Bằng chứng về tư cách công dân Hoa Kỳ có thể được thiết lập bằng cách xuất trình bản sao của bất kỳ tài liệu nào sau đây:

- Giấy khai sinh tại Hoa Kỳ hoặc Giấy Báo Sinh Lãnh Sự về việc sinh ở Nước Ngoài của một Công Dân Hoa Kỳ do Bộ Ngoại Giao Hoa Kỳ cấp;
- Hộ chiếu Hoa Kỳ;
- Giấy Chứng Nhận Nhập Tịch hoặc Giấy Chứng Nhận Tư Cách Công Dân; hoặc
- Giấy Chứng Nhận Nhập Tịch của cha mẹ quý vị cùng với giấy khai sinh của quý vị nếu quý vị trở thành công dân Hoa Kỳ do việc nhập tịch của cha mẹ quý vị.

Có một vài cách để cung cấp bằng chứng về tư cách công dân Hoa Kỳ đến văn phòng của tôi. Quý vị có thể tự tay mang đến, hoặc quý vị có thể gửi qua đường bưu điện, gửi fax, thư điện tử hoặc bằng bất kỳ phương thức truyền tải nào khác. Thông tin liên lạc của văn phòng của tôi được liệt kê ở cuối thư này.

Vui lòng cung cấp bằng chứng về tư cách công dân Hoa Kỳ trong vòng ba mươi (30) ngày kể từ ngày của bức thư này. Nếu chúng tôi không nhận được phản hồi từ quý vị trong vòng ba mươi (30) ngày, việc đăng ký cử tri của quý vị sẽ bị hủy bỏ. Trong trường hợp việc đăng ký của quý vị bị hủy, quý vị vẫn có thể được khôi phục ngay lập tức bằng cách cung cấp bằng chứng về tư cách công dân Hoa Kỳ cho văn phòng của tôi hoặc tại địa điểm bỏ phiếu của quý vị, ngay cả khi khoảng thời gian ba mươi (30) ngày đã trôi qua. Quý vị cũng có thể yêu cầu một phiên điều trần để phản đối việc hủy bỏ đăng ký của quý vị bằng cách liên hệ với văn phòng của tôi ngay cả khi quý vị không có một trong các giấy tờ trên.

Nếu quý vị có bất kỳ thắc mắc nào liên quan đến thông báo này hoặc việc đăng ký cử tri của quý vị, vui lòng liên hệ với văn phòng của tôi theo số

[REDACTED]
Quản Trị Viên phụ trách Bầu Cử

Exhibit M

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF CLAUDIO MOSSE

I, Claudio Mosse, declare as follows:

Background

1. I am over 18 years old. The statements made in this declaration are based on my personal knowledge, information, and belief.
2. I live in Nashville, Tennessee.
3. I am a member of Common Cause.

Citizenship History

4. I have been a United States citizen since 1987.
5. I was born in Santiago, Chile, in 1970. I immigrated to the United States in 1972 with my family, and grew up in the Washington, DC area.
6. I received a green card as a child. I do not recall the precise year that I received my green card.
7. I also received a Social Security Number as a child. I do not recall the precise year that I received my Social Security Number.
8. I became a naturalized United States citizen in 1987, when I was 17 years old.

9. I was issued a United States passport shortly after I was naturalized. I do not recall the precise year that it was issued.

Voting History

10. I currently live in and am registered to vote in Davidson County, Tennessee. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.

11. In order to register to vote in Tennessee, I provided the following information: name, date of birth, residential address, full Social Security Number, and telephone number.

12. I provided this information to the state of Tennessee solely to exercise my fundamental right to vote.

13. I consider this information highly private, especially my Social Security Number. When I provided this information to the state, I expected this information to remain private and securely protected.

14. I have not consented to my information being obtained, stored, or used by the federal government. Nor have I consented to the federal government sharing my information with private contractors or other third parties.

15. I deeply value my right to vote. I first registered to vote in 1988, as soon as I was eligible. I have been a registered voter ever since that time. I have regularly voted in local, state, and federal elections since I registered to vote, and I plan to continue to do so.

16. I most recently cast an early voting ballot in the May 5, 2026 primary for the August 2026 local elections. I also intend to vote in the August local elections, as well as the November midterm elections this year.

17. I strongly believe that every citizen has an obligation to help guide the actions of our government by taking part in it through their vote. If citizens do not vote, they do not have a say in their own representation and government.

18. I work to promote voter turnout and voter registration through my volunteer work. Since 2015, I have volunteered with the Tennessee Immigrant & Refugee Rights Coalition (TIRRC), a 501(c)(3) organization that organizes immigrants, refugees, and organizations that serve and support those communities, by, among other things, engaging in large-scale campaigns to help immigrants naturalize, and to register and mobilize eligible voters. From 2015 to 2016 I was a member of TIRRC's board, and from 2016 to 2024 I was the board chair. Since 2024, I have also been a board member of TIRRC Votes, the 501(c)(4) affiliate of TIRRC that also organizes immigrant and refugee communities in Tennessee and, like TIRRC, engages in large-scale campaigns to register and mobilize eligible voters. In both roles, I work to promote and lead the organizations' voter registration and mobilization efforts. I am making this declaration separate from my role in either TIRRC or TIRRC Votes.

Voting Concerns

19. It is my understanding that the Tennessee Secretary of State has provided the U.S. Department of Justice ("DOJ") with Tennessee's entire voter registration list as part of the DOJ's efforts to compile state voter data.

20. I feel that my fundamental right to vote is jeopardized by the U.S. Department of Justice ("DOJ") collecting my voter registration information.

21. I shared personal data with the state to register to vote and trusted the state to manage it accordingly.

22. I do not trust the federal government with this data. This administration has already demonstrated that it cannot accurately identify who should and should not be registered to vote. I fear that an error by the SAVE database matching system could result in me being mistakenly identified as ineligible to vote.

23. I am also concerned that there may not be a clear or timely procedure in place to notify the people whose registrations are terminated. I fear that if I were to be mistakenly identified as ineligible, I may not be notified until the day of the election when I try to vote, and that I will not have an opportunity to correct the error before I lose my ability to exercise my fundamental right to vote and participate in our government.

24. In addition, I fear that a mistake by the SAVE system might cause the Department of Homeland Security to erroneously target me for denaturalization and result in the potential loss of my citizenship.

25. I would not want the government to falsely label me a potential criminal and force me to defend myself, even if I ultimately prevailed in proving my citizenship and eligibility to vote.

Privacy Concerns

26. I feel that my privacy has been intruded on and my confidence breached by the U.S. Department of Justice (“DOJ”) collecting my voter registration information.

27. I shared personal data with the state to register to vote and trusted the state to protect it.

28. I am deeply concerned about the unification of data at the federal and state levels. Although certain agencies within the federal government already have some of my private

information, such as my Social Security Number and address, I understand that this information has been siloed within the federal government and carefully protected.

29. I believe that the consolidation of that information in one place is a serious invasion of privacy, as it allows agencies across the federal government to know much more about each of its citizens. It also creates a very attractive target for hackers and increases the chances that the data will be leaked or breached.

30. I am especially concerned about the federal government's ability to effectively secure my private data because it has failed to do so in the past. In 2015, I was employed by the federal government and was told that my Office of Personnel Management file had been hacked, possibly by a foreign entity. More recently, reports that employees of the U.S. Department of Government Efficiency committed serious security breaches involving individuals' highly sensitive personal data have continued to deepen my concern.

31. I am also deeply concerned about the possibility that DOJ is sharing my data with the Department of Homeland Security or private, third-party contractors, further increasing the possibility that my personal information will be leaked or breached.

32. Keeping my sensitive personal information private is especially important to me because I have already been targeted on the dark web. In 2025, an individual identified me by name on the dark web, claiming that I have "created problems" in Tennessee. I assume that this post was motivated by my advocacy related to immigrants' rights. The post did not identify additional sensitive personal information, such as my residential address or the names of my family members. To prevent such information from being identified and shared online by malicious actors, I used a paid privacy protection service called DeleteMe to remove those types of sensitive personally identifying information from the internet. I worry that additional leaks or

hacks that reveal my private personal information would result in additional attempts to target me and my family.

33. I am also scared that the government may deliberately misuse this data to intentionally target me for deregistration or denaturalization. I have followed this administration's efforts to denaturalize citizens, remove Temporary Protected Status from people who have no homes to return to, deport people who have claims for asylum, and arrest people on legal student visas for engaging in lawful protest. I am scared that the administration will target me because I am an immigrant and I work to support other immigrants.

34. My fear is compounded by my family's history. All four of my grandparents were German Jews who fled to Chile during World War II. Their family members who did not leave Europe were killed. My parents were both born in Chile, as was I. We immigrated to the United States in the 1970's to escape the political instability in Chile. As a result of these experiences, my family has learned over multiple generations that governments can turn on their own citizens; and that even a "good" government can quickly change. As a result, I fear that even data collected innocently may be used by another administration to persecute its citizens.

Informational Injury

35. I did not have an opportunity to comment on DOJ's decision to collect, use, and share my voter registration data. Had I been given the opportunity to comment, I would have liked to do so.

36. I regularly voice my opinion about what the government is doing and have a history of commenting on government decisions. For example, I submitted a comment to the Federal Communications Commission about a proposed rule change around 2018.

37. I would like to know why the federal government is collecting my personal voter registration data from the state.

38. I would also like to know how the government is using, or will use, my data., including what other personal information it will associate with my voter registration data, whether and how it will make voter eligibility determinations, and how its determinations will interact with the state's authority to oversee voter registration.

39. I also want to understand how the federal government will protect my private data from unauthorized access and breaches.

40. It is extremely concerning that people across the government may have access to my personal data without my consent. I am skeptical of any unauthorized national database, but especially one that contains my private data and lets government officials access and utilize it in a way that can be used against me and others similarly situated.

41. Beyond feeling violated by the disclosure of my personal information, I also feel scared. As described above, I question how secure my information is. I do not know who can access my data, and I fear that my information may be weaponized against me for political retribution or other improper purposes.

42. I will continue to encourage people to register to vote and participate in elections despite the administration's collection of voter registration data, as I deeply believe that citizens must vote to participate in government and make their voices heard. However, I wish I did not have to explain to people why they should register despite the federal government's collection of their registration data. It should not require bravery for citizens to exercise their fundamental right to vote.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 16, 2026, in Tennessee.

Claudio Mosse
Claudio Mosse

Exhibit N

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*,

Defendants.

Case No. 1:26-cv-01352-SLS

DECLARATION OF MOHAMMED NASRULLAH

I, Mohammed Nasrullah, declare as follows:

Background

1. I am over 18 years old. The statements made in this declaration are based on my personal knowledge, information, and belief.
2. I live in Houston, Texas.
3. I am a member of Common Cause of Texas.

Citizenship History

4. I have been a United States citizen since 1980.
5. I was born in Hyderabad, India, in 1952. I immigrated to the United States in August 1974 on a student visa, when I was pursuing a master's degree in nuclear engineering at the University of Oklahoma.
6. I married a United States citizen in 1976, and received my green card in 1977.
7. I was naturalized and received my United States citizenship in 1980.
8. I was issued a Social Security Number card in 1974.
9. I was issued a U.S. passport, confirming my citizenship, around 1984.

Voting History

10. I currently live in and am registered to vote in Harris County, Texas. I have not been disqualified from voting due to a felony conviction or a judgment of legal incompetence.

11. In order to register to vote in Texas, I provided the following information: name, date of birth, residential address, Texas driver's license number, telephone number, gender, voter registration number, and indication of interest in serving as an election worker.

12. I provided this information to the state of Texas solely to exercise my fundamental right to vote.

13. I consider this information highly private. When I provided this information to the state, I expected this information to remain private and securely protected.

14. I have not consented to my information being obtained, stored, or used by the federal government, or to the federal government sharing my information with private contractors or other third parties.

15. I deeply value and cherish my right to vote. I first registered to vote in 1980, as soon as I was naturalized. I have been a registered voter ever since that time. I have regularly voted in local, state, and federal elections since I registered to vote, and I plan to continue to do so.

16. I most recently voted in local elections that were held on May 2. I intend to vote in the November midterm elections this year.

17. Encouraging others to vote is a longtime passion of mine. Since 1980, I have encouraged eligible friends, neighbors, coworkers, and other community members to vote. I consider it my duty to help register as many eligible people to vote as possible.

18. I am a certified deputy voter registrar in Harris County. This role requires me to help register eligible people to vote and promote voter participation in my community.

19. Before each local, state, or federal election, I regularly send out hundreds or thousands of letters to local voters encouraging them to participate. I also organize in-person voter registration events and keep voter registration forms in my car at all times, so that I can register an eligible but unregistered person on the spot.

20. I have served as the Democratic Party precinct chair for my voting precinct since 2004. Among my most important responsibilities in that role is helping turn out voters for elections.

21. Since 2008, I have also regularly served as a presiding election judge in Democratic Party primary elections and as an alternate presiding election judge in general elections in Harris County.

Voting Concerns

22. It is my understanding that the Texas Secretary of State has provided the U.S. Department of Justice (“DOJ”) with Texas’s entire voter registration list as part of the DOJ’s efforts to compile state voter data.

23. I feel that my right to vote is jeopardized by the U.S. Department of Justice (“DOJ”) collecting my voter registration data.

24. I shared personal data with the state to register to vote and trusted the state to use it for that purpose alone.

25. I do not trust the federal government to use this personal data lawfully and appropriately. I am aware that the SAVE database has already wrongly identified eligible

registered voters as being ineligible to vote, and that people have had their registration revoked as a result.

26. I am extremely concerned that, under the terms of the Memorandum of Understanding governing Texas's sharing of its voter registration information with the federal government, Texas will accept DOJ's eligibility determinations as fact without independent investigations.

27. From my firsthand experience as an election judge, I know that when a voter's registration is revoked in Texas, the voter often receives no notice from the state. Instead, they learn that they are no longer registered only when they appear in person to cast their ballot. By then, it is too late to participate in the election even if their deregistration was in error, because Texas requires voters to register at least 30 days before an election.

28. I understand that DOJ's SAVE database is particularly likely to wrongly identify certain categories of people as ineligible to vote, including naturalized citizens. I am extremely concerned about the possibility that I, and others similarly situated to me, will be wrongly identified as ineligible to vote, and will be disenfranchised as a result.

Privacy Concerns

29. I am deeply concerned about this administration's ability to protect my personal data.

30. I am particularly concerned in light of public reporting on misconduct by employees of the U.S. Department of Government Efficiency. I have heard reports of federal employees downloading individuals' sensitive data onto their personal computers and taking it home. I am extremely concerned about this, or something like it, happening with my private

data. And I am also concerned because I know that this administration has taken many actions that courts have held to be illegal.

31. I am also deeply concerned about the possibility that DOJ is sharing my data with the Department of Homeland Security or private, third-party contractors. Every instance of sharing the data increases the possibility that my personal information will fall into the wrong hands and increases the concern that I have about what will happen with this data.

32. I am also deeply concerned that the government may misuse this data to intentionally target me for denaturalization.

33. I am aware that the current administration has sought to strip citizenship from naturalized citizens. The possibility that I may be on a list of targets keeps me up at night.

34. I fear that the current administration may target me because I am active in Democratic Party politics. I also fear becoming a target because I am a Muslim and am active in my local Muslim community. Among other things, in 2018 and 2019, I served as the president and chairman of the board of the Council on American Islamic Relations (“CAIR”) in Houston. Texas Governor Greg Abbott has proclaimed that CAIR is a terrorist organization. I am concerned that this administration may use this as a pretext to take away my citizenship or instruct Texas to terminate my voter registration.

35. While there is no legitimate basis for the government to remove my citizenship whatsoever, I nonetheless feel helpless and fearful in the face of this possibility, because I do not know how I could defend myself if that happened.

Informational Injury

36. I did not have an opportunity to comment on DOJ's decision to collect, use, and share my voter registration data. Had I been given the opportunity to comment, I would have liked to do so.

37. I regularly voice my opinion about what the government is doing and have a history of commenting on government decisions, including by offering testimony at the state legislature. Most recently, I submitted written testimony to the Texas State Board of Education last month about proposed changes to the state social studies curriculum. I also testified at the Texas State Capitol about environmental regulations in 2025. Had I been given the opportunity, I would certainly have submitted a comment here because this issue is so important and close to my heart.

38. I am anxious and concerned because I do not know what the government is doing with my data, or what steps it is taking to ensure that my data is protected.

39. I want more information about what the government is doing with my data and how it is protected from leaks, hackers, and other vulnerabilities, so that I can know if I need to do anything additional to protect my privacy.


40. It is extremely concerning that people across the government may have access to my personal data without my consent. I am skeptical of any unauthorized national database, but especially one that contains my private data and lets government officials access and utilize it in a way that can be used against me and others similarly situated.

41. Beyond feeling violated by the disclosure of my personal information, I also feel scared. As described above, I question how secure my information is. I do not know who can

access my data, and I fear that my information may be weaponized against me for political retribution or other improper purposes.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Executed on May 15, 2026, in Texas.


Mohammed Nasrullah

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE, *et al.*

Plaintiffs,

v.

U.S. DEPARTMENT OF JUSTICE, *et al.*

Defendants.

Case No. 1:26-cv-01352-SLS

[PLAINTIFFS' PROPOSED] ORDER

Upon consideration of Plaintiffs' Motion for Partial Summary Judgment, Defendants' cross-dispositive motion, and the entire record in this case, the Court concludes that Plaintiffs are entitled to judgment as a matter of law as to Counts I, VI, VII, and VIII.

Accordingly, it is hereby ordered that Plaintiffs' Motion for Partial Summary Judgment is **GRANTED**. It is further **ORDERED** that Defendants' cross-dispositive motion is **DENIED**.

It is further **DECLARED** that the Department of Justice's ("DOJ's") Voter List Maintenance Policy, as well as associated policies and agreements, are unlawful and violate the Administrative Procedure Act.

It is further **ORDERED** that:

1. DOJ's Voter List Maintenance Policy, as well as associated policies and agreements, are vacated and set aside.
2. Defendants Acting U.S. Attorney General Todd Blanche, DOJ, and their officers, agents, servants, employees, and attorneys, and all persons acting in concert or participation with them—including but not limited to the Department of Homeland Security ("DHS"), U.S. Citizenship and Immigration Services ("USCIS"), and Homeland Security Investigations

(“HSI”)—shall immediately cease all maintenance, collection, use, or disclosure of statewide voter registration list (“SVRL”) data under the Voter List Maintenance Policy.

3. Defendants Acting U.S. Attorney General Todd Blanche, DOJ, and their officers, agents, servants, employees, attorneys, and all persons acting in concert or participation with them—including but not limited to DHS, USCIS, and HSI—shall, within two weeks of this order, delete, disentangle, and unlink any SVRL data in their possession, custody or control.
4. Defendants Acting U.S. Attorney General Todd Blanche, DOJ, and their officers, agents, servants, employees, and attorneys, and all persons acting in concert or participation with them—including but not limited to DHS, USCIS, and HSI—shall, within two weeks of this order, instruct any party they have provided SVRL data to delete, disentangle and unlink such data.
5. Defendants Acting U.S. Attorney General Todd Blanche, DOJ, and their officers, agents, servants, employees, and attorneys, and all persons acting in concert or participation with them—including but not limited to DHS, USCIS, and HSI—shall, within two weeks of this order, withdraw all memoranda of understanding, policies, and other agreements related to the Voter List Maintenance Policy.
6. Defendants Acting U.S. Attorney General Todd Blanche and DOJ shall immediately provide notice of this order and its requirements to all of DOJ’s officers, agents, servants, employees, and attorneys, and all persons acting in concert or participation with DOJ—including but not limited to DHS, USCIS, and HSI.

7. Defendants Acting U.S. Attorney General Todd Blanche and DOJ shall, within three weeks of entry of this order, file a status report with the Court describing the steps it has taken to comply with this order.

SO ORDERED.

DATED this ____ day of _____, 2026.

Hon. Sparkle L. Sooknanan
United States District Judge