

IN THE
Supreme Court of the United States

DEPARTMENT OF HOMELAND SECURITY, ET AL.,
Applicants,

v.

LEAGUE OF WOMEN VOTERS, ET AL.,
Respondents.

ON APPLICATION TO STAY THE ORDER OF
THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

**BRIEF OF LAWYERS DEFENDING AMERICAN DEMOCRACY
AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENTS**

Gary DiBianco
LAWYERS FOR GOOD GOVERNMENT
1319 F St. NW, Suite 301, PMB 181
Washington, DC 20004
(404) 913-5529
gary@lawyersforgoodgovernment.org
Counsel of Record

TABLE OF CONTENTS

TABLE OF CONTENTS.....	i
TABLE OF AUTHORITIES	ii
INTEREST OF <i>AMICUS CURIAE</i> LAWYERS DEFENDING AMERICAN DEMOCRACY	1
SUMMARY OF ARGUMENT	2
ARGUMENT	3
I. Statutory and Regulatory Prohibitions on Disclosure Reflect the Sensitivity of SSNs	3
A. <i>The Social Security Act Strictly Limits the Disclosure of SSNs and SSA Records</i>	3
B. <i>The Privacy Act of 1974 Prohibits Disclosure of SSNs and SSA Records</i> ...	5
C. <i>The Prohibition on Disclosure in § 405(c)(2)(C)(viii)(I) Applies to the Modified SAVE Program</i>	9
II. SSA’s Citizenship Data is Inaccurate.....	13
III.A National Database Creates Significant Security Risks	14
CONCLUSION.....	16

TABLE OF AUTHORITIES

STATUTES

42 U.S.C. § 1306(a)	4, 5
42 U.S.C. §§ 301-304 (1935)	3
52 U.S.C. § 20507	9
52 U.S.C. § 21083(a)	9
8 U.S.C. § 1360(c)	9
8 U.S.C. § 1360(b)	8
8 U.S.C. § 1373(c)	8
Deficit Reduction Act of 1984, Pub. L. No. 98-369, 98 Stat. 494	8
Omnibus Budget Reconciliation Act of 1981, Pub. L. No. 97-35, 95 Stat. 357.....	8
Pub. L. No. 96-58, 93 Stat. 389.....	8
Social Security Amendments of 1981, Pub. L. No. 97-123, 95 Stat. 1659.....	8
Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520.....	7

OTHER

Admin. Office of the U.S. Courts, Cybersecurity Measures Strengthened in Light of Attacks on Judiciary's Case Management System (Aug. 7, 2025), https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system [https://perma.cc/NX6L-P2KK]	15
<i>American Fed’n of State, Cnty. & Mun. Emps., AFL-CIO v. Soc. Sec. Admin.</i> , No. 1:25-cv-00596-ELH (E.D. Va. Jan. 16, 2026), ECF No.197	16
Barbara McQuade, <i>Comment: DOJ’s voter info demand a data breach waiting to happen</i> (Jan. 13, 2026), https://www.heraldnet.com/2026/01/13/comment-dojs-voter-info-demand-a-data-breach-waiting-to-happen/	15
E-mail from Dana L. Gold & Andrea Meza, Att’ys, Gov’t Accountability Project, to Hon. Rand Paul, Chair, & Hon. Gary Peters, Ranking Member, S. Comm. on Homeland Sec. & Governmental Affairs, <i>et al.</i> (Aug. 26, 2025) (on file with the Government Accountability Project), https://whistleblower.org/wp-content/uploads/2025/08/08-26-2025-Borges-Disclosure-Sanitized.pdf	16
E-mail from Nancy Morales Gonzalez, Assoc. Gen. Counsel for Gen. Law, Div. 1, Soc. Sec. Admin., to Jon Sherman, Litig. Dir. & Senior Counsel, Fair Elections Ctr. (July 13, 2023) (on file with the Fair Elections Center), https://perma.cc/KS2N-U2US	13, 14

Fatima Hussein, <i>Social Security watchdog opens probe into alleged misuse of data by ex-DOGE employee</i> , AP News (Mar. 11, 2026), https://apnews.com/article/social-security-administration-data-breach-privacy-doge-69ca1f69fee8633c91655771059cb50d	16
Info. Sec. Oversight Office, Memorandum for the Senior Agency Official for the Controlled Unclassified Information (CUI) Program at the U.S. Department of Homeland Security 3 (Sept. 7, 2018)	5
Kevin Collier, <i>Social Security Number Leaked? Chances Are, a Criminal is Already Trying to Use It</i> , ABC (Aug. 4, 2025), https://www.nbcnews.com/tech/security/security-numbers-leaked-personal-data-puts-people-high-risk-identity-rcna221452	15
Meryl Kornfield, Elizabeth Dwoskin, & Lisa Rein, <i>Whistleblower claims ex-DOGE member says he took Social Security data to new job</i> , The Washington Post (Mar. 10, 2026), https://www.washingtonpost.com/politics/2026/03/10/social-security-data-breach-doge-2/	16
Office of Inspector Gen., Soc. Sec. Admin., Congressional Response Report, Accuracy of the Social Security Administration's Numident File, A-08-06-26100 (Dec. 2006), https://perma.cc/5G2J-FF4V	14
Office of Mgmt. & Budget, Exec. Office of the President, Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)	14
Press Release, U.S. Dep't of Justice, <i>Two Virginia Men Arrested for Conspiring to Destroy Government Databases</i> (Dec. 3, 2025), https://www.justice.gov/opa/pr/two-virginia-men-arrested-conspiring-destroy-government-databases [https://perma.cc/JP2T-3ZQY].....	15
Sandy Crank, <i>The Evolution of Privacy and Disclosure Policy in the Social Security Administration</i> , Soc. Sec. Bull., Jun. 1985.....	4
Soc. Sec. Admin., POMS GN 03325.002, Disclosure and Verification of Social Security Numbers (SSN) Without Consent (2023)	5
Statement of Sen. Sam Ervin, June 11, 1974, Legislative History of the Privacy Act of 1974, S. Comm. on Gov't Operations & Subcomm. on Gov't Info. & Individual Rights of the H. Comm. on Gov't Operations, 94th Cong., Source Book on Privacy 157 (1976).....	6
Understanding The Importance Of Data Segregation And Access Control, DataBank (July 6, 2024), https://www.databank.com/resources/blogs/understanding-the-importance-of-data-segregation-and-access-control/	15

REGULATIONS

20 C.F.R. §§ 401.5-401.95	5
Soc. Sec. Bd., Reg. No. 1 (June 15, 1937)	4

INTEREST OF *AMICUS CURIAE*
LAWYERS DEFENDING AMERICAN DEMOCRACY¹

Lawyers Defending American Democracy (LDAD) is a non-profit, non-partisan organization devoted to encouraging the legal profession to protect and preserve democracy and the rule of law. LDAD's Board includes a retired state Supreme Court Chief Justice, a former state Attorney General, former state bar officers, current and former corporate counsel, current law professors, and a former major law firm managing partner.

LDAD has a significant interest in this case because the large-scale acquisition and disclosure by the Department of Homeland Security (DHS) of Social Security numbers (SSNs) and related records violates statutes that protect the confidentiality of this uniquely sensitive personal information. Furthermore, the attempted use of this information by the executive branch to assemble a national database is precisely what Congress sought to prevent in enacting these statutes. In this case, a database designed to compile a putative official record of eligible voters would create an especially significant risk because it could be used by the executive in ways that would pose a significant risk to the rule of law and our constitutional democracy.

LDAD's brief makes a distinctive contribution to this proceeding by describing for the Court the legislative history of statutes restricting the disclosure of Social

¹ No counsel for a party authored the brief in whole or in part and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief.

Security numbers and related records, and the Congressional concerns that have animated this deliberate statutory regime.

LDAD sought the consent of all Parties prior to filing this Brief in support of Respondents. Respondents consented to this filing, and Applicants stated that they take no position with respect to it.

SUMMARY OF ARGUMENT

Strict limits on disclosure of SSNs and other related information have been in effect since the very beginning of the Social Security program. The first regulation of the Social Security Board prohibited disclosure of this information. This was later codified in what is now 42 U.S.C. §1306, which contains limited exceptions to the prohibition. The Privacy Act of 1974, codified at 5 U.S.C. § 552a(b), supplements these restrictions. Together, these statutes prohibit disclosure of SSNs and related records unless explicitly authorized by law.

Applicants claim that 8 U.S.C. §1373 authorizes the modified Systemic Alien Verification for Entitlements (SAVE) program at issue in this case. That statute, however, merely authorizes acquisition by DHS of information regarding immigration. It contains no explicit authorization for the use of SSNs or related records. Applicants therefore are subject to the prohibitions on disclosure in at 42 U.S.C. § 1306 and 5 U.S.C. § 552a(b). As this brief describes, statutes that do authorize disclosure of information to DHS are far more circumscribed and limited in what they authorize than the use to which DHS seeks to put them for the modified SAVE program.

Applicants also presented an argument only after summary judgment that the modified SAVE program is authorized by 42 U.S.C. § 405(c)(2)(C)(viii)(I), which the Court of Appeals appropriately regarded as forfeited. If this Court nonetheless decides to consider that argument, our brief sets forth the legislative history of that subsection, which demonstrates that the government misunderstands the origin and purpose of that provision. This history indicates that the prohibition in this subsection plainly applies to the modified SAVE program.

It is also important to appreciate that the Social Security Administration (SSA) itself recognizes that its records are incomplete and unreliable in confirming current U.S. citizenship. The use of SSNs and related records to compile a national database is problematic enough, but doing so to comprise an inaccurate database that purports to establish voter eligibility poses an especially grave risk to the rule of law and the electoral system in our constitutional democracy. The significant vulnerability of a centralized national voter database risks to cybersecurity attacks and widescale identity-theft compounds this risk.

ARGUMENT

I. STATUTORY AND REGULATORY PROHIBITIONS ON DISCLOSURE REFLECT THE SENSITIVITY OF SSNS

A. The Social Security Act Strictly Limits the Disclosure of SSNs and SSA Records

The Social Security Act of 1935 (Act) created SSNs to assist in providing benefits such as retirement and unemployment income. 42 U.S.C. §§ 301-304 (1935). The strict confidentiality of SSA records has been a crucial feature of the Social

Security program from the outset. On June 15, 1937, the first regulation adopted by the Social Security Board flatly prohibited any “member, officer, or employee of the Board” from producing or disclosing “any record . . . or any information acquired therefrom . . . pertaining to any person.” Soc. Sec. Bd., Reg. No. 1 (June 15, 1937). Indeed, employees were directed to decline disclosure even when “sought to be required, by subpoena or other compulsory process.” *Id.*

The Social Security Board, through Regulation No. 1, originally restricted disclosure to just three categories of recipients, each related to benefits under the Act: (1) a claimant or prospective beneficiary under the Act; (2) Treasury Department officers administering the Act; and (3) state officials administering unemployment compensation laws. *Id.* The initial disclosure rule applied to “any record . . . or any information acquired therefrom or otherwise officially acquired,” thus making clear that *all* information obtained by the SSA was considered private, sensitive, and confidential. *Id.*

Congress amended the Social Security Act in 1939 and codified Regulation Number 1 in 42 U.S.C. § 1306, the foundational statute that governs disclosure of SSNs and SSA records. *See* Social Security Act Amendments of 1939, § 1106, 53 Stat. 1360. Section 1306 prohibits the disclosure of “any file, record, report, or other paper, or any information” except as agency regulations prescribe and as “otherwise provided by Federal law.” 42 U.S.C. § 1306(a).²

² *See* Sandy Crank, *The Evolution of Privacy and Disclosure Policy in the Social Security Administration*, Soc. Sec. Bull., Jun. 1985, at 9.

SSA regulations reinforce this prohibition,³ as does the SSA Program Operations Manual System (POMS).⁴ The Manual explains that “[b]ecause of the sensitivity of the SSN as a unique personal identifier, we only verify SSNs without consent” if “a Federal law requires us to verify SSNs; a Federal law authorizes the collection of SSNs to administer an income/health maintenance program, allowing us to verify SSNs to the agency administering the program; or one or more of the Privacy Act’s disclosure exceptions allows us to verify SSNs.” Soc. Sec. Admin., POMS GN 03325.002, *supra*, Section A. A statute “must specifically mandate that SSA disclose SSNs” for the SSA to disclose them. *Id.*, Section B.1.

The Manual explicitly states, “We do not have the legal authority to disclose information about U.S. citizens to DHS.”⁵ The federal government classifies SSNs as “stand-alone” sensitive personally identifiable information (PII), meaning the disclosure of SSNs can cause substantial harm even when not combined with other data.⁶

B. The Privacy Act of 1974 Prohibits Disclosure of SSNs and SSA Records

By 1974, SSNs were used for various purposes, including tax reporting by banks, service identification by the military, driver’s licenses, welfare programs, and

³ See 42 U.S.C. § 1306(a); 20 C.F.R. §§ 401.5-401.95 (implementing the Privacy Act of 1974, *infra*, Section I.B).

⁴ Soc. Sec. Admin., POMS GN 03325.002: Disclosure and Verification of Social Security Numbers (SSN) Without Consent (2023).

⁵ *Id.*, at (D)(1).

⁶ See Info. Sec. Oversight Office, Memorandum for the Senior Agency Official for the Controlled Unclassified Information (CUI) Program at the U.S. Department of Homeland Security 3 (Sept. 7, 2018); see discussion *infra* Section III.B.

tax administration by states. The Privacy Act of 1974 (Privacy Act) was enacted explicitly to address the risk to privacy posed by this proliferation.⁷ It also restricts the disclosure of SSNs.

During Senate hearings Senator Sam Ervin discussed the urgent need for the bill:

[T]his is a *bipartisan issue* which [a]ffects people in all walks of life. *The complaints have shown that despite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information-gathering tactics and its technical capacity to store and distribute information.*

When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.

The complaints show that many Americans are more concerned than ever before about what might be in their records because Government has abused, and may abuse, its power to investigate and store information. *They are concerned about the transfer of information from data bank to data bank and black list to black list because they have seen instances of it.*⁸

⁷ See Legislative History of the Privacy Act of 1974, S. Comm. on Gov't Operations & Subcomm. on Gov't Info. & Individual Rights of the H. Comm. on Gov't Operations, 94th Cong., Source Book on Privacy at 61 (1976).

⁸ Statement of Sen. Sam Ervin, June 11, 1974, Legislative History of the Privacy Act of 1974, S. Comm. on Gov't Operations & Subcomm. on Gov't Info. & Individual Rights of the H. Comm. on Gov't Operations, 94th Cong., Source Book on Privacy at 157 (1976) (emphasis added).

During those same hearings, Arthur R. Miller, a distinguished Harvard Law School professor and an expert in privacy, technology, and computers, warned of the “spread of the databank concept” because of its serious risks:

The information gathering and surveillance activities of the Federal Government have expanded to such an extent that they are becoming a threat to several of every American’s basic rights, the rights of privacy, speech, assembly, association, and petition of the Government. . . .

*In the past, dictatorships always have come with hobnailed boots and tanks and machine guns, but a dictatorship of dossiers, a dictatorship of data banks can be just as repressive, just as chilling and just as debilitating on our constitutional protections. I think it is this fear that presents the greatest challenge to Congress right now.*⁹

Senator Henry M. “Scoop” Jackson expressed similar fears: “We are concerned with the danger of this sort of system being institutionalized to the point where it can all be fed into one central system in which there could be a misuse of that information.”¹⁰

Since the passage of the Privacy Act, Congress has authorized disclosure of SSNs primarily in connection with eligibility for federal benefits. Thus, Congress amended the Social Security Act in 1976 to allow states to use SSNs for four specific purposes: (1) the administration of taxation; (2) public assistance; (3) driver’s license registration; and (4) motor vehicle registration, and made the unlawful or compelled disclosure of SSNs a felony.¹¹ Subsequent enactments allowed disclosure in

⁹ Statement of Prof. Arthur Miller, *id.* at 160 (emphasis added).

¹⁰ Statement of Henry “Scoop” Jackson, *id.* at 57.

¹¹ Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520.

connection with federal benefits such as the food stamp program; the school lunch program;¹² suspension of disability benefits to convicted felons while incarcerated;¹³ and eligibility for Medicaid, unemployment compensation, food stamps and benefits under the Aid to Families with Dependent Children (AFDC) program.¹⁴

The modified SAVE program represents precisely the type of centralized database that Congress sought to prevent with the Privacy Act. The Privacy Act specifically prohibits disclosure of SSNs and related information “except pursuant to a *written request by, or with the prior written consent of*, the individual to whom the record pertains” subject only to closely circumscribed exceptions. 5 U.S.C. § 552a(b) (emphasis added).

When Congress has authorized SSA disclosures to DHS, it has created clear limitations. For example, the Immigration and Nationality Act (INA), which requires SSA to disclose to DHS “information concerning the identity and location of *aliens* in the United States” when requested, applies only to *aliens*. 8 U.S.C. § 1360(b) (emphasis added). INA does not authorize the SSA to disclose information about *U.S. citizens* to DHS. 8 U.S.C. § 1373(c). Further, the SSN may be disclosed only for *verification* purposes, that is, to confirm DHS information about aliens. *Id.* The INA does not allow the SSA to feed SSNs and citizenship information into a mass data-bank to check voter eligibility.

¹² Pub. L. No. 96-58, 93 Stat. 389 (Omnibus Budget Reconciliation Act of 1981, Pub. L. No. 97-35, 95 Stat. 357).

¹³ Social Security Amendments of 1981, Pub. L. No. 97-123, 95 Stat. 1659.

¹⁴ Deficit Reduction Act of 1984, Pub. L. No. 98-369, 98 Stat. 494.

Similarly, the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 authorizes the SSA to disclose to DHS “certain information concerning *an alien* to whom [SSA] issued an SSN for non-work purposes and for whom earnings are reported.” 8 U.S.C. § 1360(c)(2) (emphasis added). The statute specifically limits the disclosure to the name and address of the *alien*, the employer and the amount of earnings. *Id.* It does not authorize the mass disclosure of SSNs or any disclosure of the SSNs of U.S. citizens.

Moreover, the Help America Vote Act of 2002 (HAVA) permits *state election boards* to verify voter eligibility with SSA, but only as a secondary source when the state cannot verify registration information through state motor vehicle records. 52 U.S.C. § 20507. Even that verification is restricted to the last four digits of the SSN. 52 U.S.C. § 21083(a)(5)(B).

C. The Prohibition on Disclosure in § 405(c)(2)(C)(viii)(I) Applies to the Modified SAVE Program

The Court of Appeals appropriately held that Applicants had forfeited the argument that the prohibition on disclosure of SSNs and related records under 42 U.S.C. § 405(c)(2)(C)(viii)(I) does not apply to the modified SAVE program, because Applicants raised this argument for the first time after summary judgment and declined the District Court’s invitation to file a post-judgment motion to request the court to excuse the forfeiture and consider the argument. To the extent this Court nonetheless considers Applicants’ argument regarding 42 U.S.C. § 405(c)(2)(C)(viii)(I) that were not briefed below, that argument fails because

Applicants do not understand the specific context in which that provision was added to the Social Security Act. In so doing, they ignore the way in which Congress intended this subsection to reinforce strict disclosure limitations of 42 U.S. C. § 1306.

42 U.S.C. §405(c)(2)(C)(viii)(I) states:

Social security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law enacted on or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such social security account number or related record.

Applicants have argued that “SSA’s disclosure of information to DHS does not violate Section 405(c)(2) [because] [t]he cited clause by its own terms, protects only numbers and related records that were ‘obtained or maintained . . . pursuant to any provision of law enacted *on or after October 1, 1990.*’” *See Applicants’ Application*, p. 30-31 (emphasis in original) [citations omitted].

The legislative history of this subsection, however, indicates that it was plainly intended to cover the disclosure by DHS at issue in this case, 42 U.S.C. § 405(c)(2)(C)(viii)(I) was enacted as part of the Food, Agriculture, Conservation and Trade Act of 1990 (FACT Act of 1990) Pub. L. No. 101-624, tit. XXII, § 2201(c), Nov. 28, 1990, 104 Stat. 3952. Title XXII Section 2201 of the FACT Act amended the Federal Crop Insurance Act, 7 U.S.C. §1506, to provide federal assistance to farmers seeking crop insurance and disaster relief. This portion of the FACT Act required farmers seeking such federal assistance to disclose their social security numbers to

the Federal Crop Insurance Corporation as part of the application process. It provided:

(a) SUBMISSION REQUIRED. – Section 506 of the Federal Crop Insurance Act (7 U.S.C. 1506) is amended by adding at the end of the following new subsection:

“(I) SUBMISSION OF CERTAIN INFORMATION. –

(1) SOCIAL SECURITY ACCOUNT AND EMPLOYER IDENTIFICATION NUMBERS. – The (Federal Crop Insurance) Corporation shall require, as a condition of eligibility for participation in the multiple peril crop insurance program, submission of the social security numbers”

See Pub. L. No. 101-624, tit. XXII, § 2201(a) (emphasis added).

The Social Security Act was also amended in the same Bill for the specific purpose of protecting the privacy and confidentiality of program applicants’ social security information by prohibiting re-disclosure of the applicants’ Social Security information that they were required to submit to the Corporation. The bill therefore amended Section 205 (c) (2) (C) of the Social Security Act, 42 U.S.C. § 405(c)(2)(C), to

include a new subsection, (vii)(I) (now subsection (viii)(I)), to address the confidentiality, privacy and non-redisclosure of such information:

(c) CONFIDENTIALITY OF SOCIAL SECURITY ACCOUNT NUMBER. –

Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C) (as amended by subsection (b)) is further amended by adding at the end thereof the following clause:

“(vii)(I) Social security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law enacted on or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such social security account number or related record.”

See Pub. L. No. 101-624, tit. XXII, § 2201(c) (emphasis added).

The October 1, 1990, date in this provision thus was meant to refer to the application of this disclosure restriction after enactment of this legislation. The clear intention of Congress in amending the Social Security Act to include § 405(c)(2)(C)(viii)(I) therefore was to augment the confidentiality of SSN’s already set forth in 42 U.S.C. §1306, and to provide protection against disclosure of SSNs specifically because Title XXII, § 2201(a), required the disclosure of SSNs by farmers applying for assistance. That mandatory disclosure was, itself, a departure from the confidentiality provisions of § 1306. The Social Security Act was amended to include § 405(c)(2)(C)(viii)(I) to bring Title XXII in line with existing law prohibiting disclosure of SSN’s as codified in 42 U.S.C. §1306. Thus, any SSN obtained or maintained after October 1, 1990, could not be disclosed under the provisions of § 405(c)(2)(C)(viii)(I). Any information obtained or maintained by authorities prior to

that date could not be disclosed under 42 U.S.C. §1306. Applicants therefore are incorrect that 42 U.S.C. § 405(c)(2)(C)(viii)(I) does not prohibit disclosure of SSNs and related records under the modified SAVE program. As we have explained, DHS's claim that 8 U.S.C. § 1373 authorizes it to establish the modified SAVE program is inaccurate, but in any event, that statute was adopted in 1996—well after the October 1, 1990, date specified in § 405(c)(2)(C)(viii)(I).

II. SSA'S CITIZENSHIP DATA IS INACCURATE

SSNs are not accurate or reliable sources of information about citizenship status. It is DHS that has the most up-to-date and accurate information concerning immigration and citizenship status of non-citizens.

As a practical matter, the SSA does not gather or maintain information to determine citizenship. Rather, SSA records reflect citizenship status only as of the date of application for benefits or an SSN, not current citizenship status. SSA records are not automatically updated for those who become naturalized citizens after they already have their SSNs. Indeed, the SSA's Office of the General Counsel has recognized that “[w]hile SSA records provide an indication of citizenship, they do not provide definitive information on U.S. citizenship.”¹⁵ Further, the SSA only began “to consistently maintain citizenship information” in 1981 and persons are not required to update their information except under limited circumstances (receipt of

¹⁵ E-mail from Nancy Morales Gonzalez, Assoc. Gen. Counsel for Gen. Law, Div. 1, Soc. Sec. Admin., to Jon Sherman, Litig. Dir. & Senior Counsel, Fair Elections Ctr. (July 13, 2023) (on file with the Fair Elections Center), at 2, <https://perma.cc/KS2N-U2US>.

benefits or request for a replacement card). *Id.* As a result, SSA records merely reflect an outdated snapshot of citizenship status at a single point in time. SSA therefore “does not have citizenship information for all individuals who have been issued an SSN.” *Id.*

Moreover, the SSA Inspector General (IG) has expressed concern “with the extent of incorrect citizenship information in SSA’s Numident [Numerical Identification System] file for [] foreign-born U.S. citizens and non-U.S. citizens.”¹⁶ The IG found that 7.0% of people identified as non-U.S. citizens were actually U.S. citizens. *Id.* In addition, “of the 46.5 million non-U.S. citizen records” estimated to be in SSA’s files, “about 3.3 million contain incorrect citizenship status codes.” *Id.* at 13. In sum, the SSA’s database is not intended to be—and in fact is not—a reliable source of information on citizenship status, particularly regarding naturalized citizens. The risks associated with bulk disclosure to DHS or inclusion of SSNs in a SAVE database thus far outweigh any conceivable benefit, and risk disenfranchising millions of U.S. citizens.

III. A NATIONAL DATABASE CREATES SIGNIFICANT SECURITY RISKS

The federal government classifies any full or partial SSN as “Personally Identifiable Information” that increases identity theft risks.¹⁷ The SAVE database,

¹⁶ Office of Inspector Gen., Soc. Sec. Admin., Congressional Response Report, Accuracy of the Social Security Administration's Numident File, A-08-06-26100 (Dec. 2006), <https://perma.cc/5G2J-FF4V>, at ii.

¹⁷ Office of Mgmt. & Budget, Exec. Office of the President, Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).

with multiple millions of social security numbers and other information, would be vulnerable to cybersecurity attacks and widescale identity theft. The practice of segregating data in order to restrict access to those with a legitimate need to know is a bedrock principle of information security. To this point, Barbara McQuade, former national security prosecutor, has observed, “A single breach of a database that contains both driver’s license and Social Security numbers could enable identity theft on a massive scale.”¹⁸ The SAVE overhaul creates such a risk.

Data breaches unfortunately are all too common. The Identity Theft Resource Center documented 1,857 data breaches involving Americans’ SSNs in 2024 and the FTC received 1.1 million claims of identity theft.¹⁹ In January 2026, researchers detected an exposed database with approximately 2.7 billion records containing Social Security numbers.²⁰ In December 2025, government contractors were charged in an insider data breach affecting multiple federal agencies.²¹ A centralized

¹⁸ See Barbara McQuade, *Comment: DOJ’s voter info demand a data breach waiting to happen* (Jan. 13, 2026),

www.heraldnet.com/2026/01/13/comment-dojs-voter-info-demand-a-data-breach-waiting-to-happen/; see also Understanding The Importance Of Data Segregation And Access Control, DataBank (July 6, 2024), www.databank.com/resources/blogs/understanding-the-importance-of-data-segregation-and-access-control/.

¹⁹ Kevin Collier, *Social Security Number Leaked? Chances Are, a Criminal is Already Trying to Use It*, ABC (Aug. 4, 2025), www.nbcnews.com/tech/security/security-numbers-leaked-personal-data-puts-people-high-risk-identity-rcna221452.

²⁰ Greg Pollock, *Social Insecurity: Billions of Social Security Number [sic] and Passwords*, UpGuard (Feb. 18, 2026),

www.upguard.com/breaches/social-insecurity-billions-of-social-security-number-and-passwords

²¹ Press Release, U.S. Dep’t of Justice, *Two Virginia Men Arrested for Conspiring to Destroy Government Databases* (Dec. 3, 2025), <https://www.justice.gov/opa/pr/two-virginia-men-arrested-conspiring-destroy-government-databases> [<https://perma.cc/JP2T-3ZQY>]; Admin. Office of the U.S. Courts, *Cybersecurity Measures Strengthened in Light of Attacks on Judiciary’s Case Management System* (Aug. 7, 2025), <https://www.uscourts.gov/data-news/judiciary-news/2025/08/07/cybersecurity-measures-strengthened-light-attacks-judiciarys-case-management-system>; [<https://perma.cc/NX6L-P2KK>] (federal judiciary case management system breached).

database will inevitably be targeted by cybersecurity attacks, exposing the sensitive personal information of millions of people to theft and other misuse.

Indeed, since the overhaul of the SAVE system began, several whistleblowers have reported the Department of Government Efficiency's (DOGE) mishandling of SSA Numident data. The DOJ has acknowledged that some DOGE employees failed to safeguard this information and that "members of SSA's DOGE Team were using links to share data through the third-party server 'Cloudflare,'" which "is not approved for storing SSA data and when used in this manner is outside SSA's security protocols."²² The DOJ does not know "exactly what data were shared to Cloudflare or whether the data still exist on the server." *Id.* And the SSA's IG apparently is also investigating a whistleblower claim that a former DOGE member sought to download the SSA Numident database to a thumb drive for use at his new job.²³

CONCLUSION

For the reasons stated above, Lawyers Defending American Democracy respectfully requests that this Court deny Applicants' Application to Stay the Order of the United States District Court for the District of Columbia.

²² *American Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. Soc. Sec. Admin.*, No. 1:25-cv-00596-ELH (E.D. Va. Jan. 16, 2026), ECF No.197, at 6.

²³ Meryl Kornfield, Elizabeth Dwoskin, & Lisa Rein, *Whistleblower claims ex-DOGE member says he took Social Security data to new job*, The Washington Post (Mar. 10, 2026), <https://www.washingtonpost.com/politics/2026/03/10/social-security-data-breach-doge-2/>; Fatima Hussein, *Social Security watchdog opens probe into alleged misuse of data by ex-DOGE employee*, AP News (Mar. 11, 2026), <https://apnews.com/article/social-security-administration-data-breach-privacy-doge-69ca1f69fee8633c91655771059cb50d>.

Dated: September 14, 2026

Respectfully submitted,
LAWYERS DEFENDING AMERICAN
DEMOCRACY,
by its counsel,

/s/ Gary DiBianco
Gary DiBianco
LAWYERS FOR GOOD GOVERNMENT
1319 F St. NW, Suite 301, PMB 181
Washington, DC 20004
(404) 913-5529
gary@lawyersforgoodgovernment.org
Counsel of Record