UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LEAGUE OF WOMEN VOTERS, *et al.*,	*	
	*	
Plaintiffs,	*	
	*	
v.	*	**Case No. 25-cv-3501-SLS**
	*	
U.S. DEPARTMENT OF HOMELAND SECURITY, *et al.*,	*	
	*	
	*	
Defendants.	*	
	*	

MEMORANDUM OF AMICUS
LAWYERS DEFENDING AMERICAN DEMOCRACY
IN SUPPORT OF
PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Other Authorities

IDENTITY AND INTEREST OF AMICUS

Lawyers Defending American Democracy (LDAD) files this amicus brief in support of Plaintiffs' Motion for Summary Judgment. LDAD is a non-profit, non-partisan organization devoted to encouraging the legal profession to enforce and to uphold democracy and the rule of law consistent with our obligations as lawyers, demanding accountability from lawyers and public officials, and identifying attacks on legal norms and prescribing redress for them. LDAD has a significant interest in this case because the large-scale disclosure of Social Security Numbers is unauthorized by Congress, fundamentally contrary to Congressional intent, and poses a grave risk that compilation of such sensitive personal information into a massive database can be misused by the executive branch without either awareness of the public or democratic accountability. Plaintiffs have consented to our filing this brief. The Defendants take no position with respect to our filing this brief. A motion for leave to file is attached.

SUMMARY OF ARGUMENT

Congress has historically treated the disclosure of personal Social Security information, particularly Social Security Numbers (SSNs), with immense caution. The overhaul of the Systemic Alien Verification Database (SAVE) through the integration of SSNs that was initiated by Executive Order (EO) 14248—purportedly to reduce voter fraud—is an extreme departure from longstanding statutory and

administrative practice designed to ensure strict limitations on disclosure of this uniquely sensitive personal information. Exec. Order No. 14,248, 90 Fed. Reg. 14005. Put simply, widespread sharing of highly confidential SSNs is not lawful.

Historically, when Congress has passed legislation permitting the Social Security Administration (SSA) to share SSNs, it has done so by crafting specific, narrow rules. This reflects the intention to limit disclosure of this uniquely sensitive information to exceptional circumstances. Furthermore, there is no basis for including the SSNs of U.S.-born citizens in a database maintained by the Department of Homeland Security (DHS)—an agency whose mission is "safeguarding the American people." https://www.dhs.gov/we-are-dhs.

Moreover, the inclusion of this information is unsuited for DHS's stated purpose, since even the SSA acknowledges that its own records are unreliable and incomplete when it comes to confirming current U.S. citizenship. In cases in which voters have challenged the use of SSNs to prevent voter fraud, courts have rejected the federal government's argument that it needs to gather and use confidential SSA information for this purpose.

Finally, the consolidation of SSNs in a single national database creates significant security risks for individuals. Millions of SSNs are now vulnerable to cybersecurity attacks and widescale identity theft. They are also at risk of being

used by the executive branch to target individuals for political, personal, or other improper reasons.

ARGUMENT

I. Statutory and Regulatory Prohibitions on Disclosure Reflect the Sensitivity of Social Security Numbers

A. Congress Created the SSN for a Narrow Purpose and Immediately Imposed Strict Confidentiality Requirements

The Social Security Act of 1935 was created to provide economic assistance through benefit programs such as retirement and unemployment income. SSNs were established as an administrative tool for the SSA to provide these benefits to those who qualified. 42 U.S.C. §§ 301-304 (1935).

The privacy and confidentiality of SSA records has been recognized as a crucial feature of the Social Security program from the outset. On June 15, 1937, the very first regulation adopted by the Social Security Board underscored the confidential nature of records collected under the Act. The regulation 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). The importance of confidentiality was so essential that employees were directed to decline disclosure even when "sought to be required, by subpoena or other compulsory process." *Id*.

Congress originally authorized information disclosures related to only three categories of recipients, each related to benefits under the Act: (1) a claimant or prospective claimant for benefits under the Act; (2) Treasury Department officers administering the Act; and (3) state officials administering unemployment compensation laws. *Id.* The plain language of the initial disclosure rule—"any record… or any information acquired therefrom or otherwise officially acquired"—makes clear that *all* information obtained by SSA was considered private, sensitive, and confidential. Congress codified the language of Regulation Number 1 in its 1939 amendments to the Social Security Act at §1106: the Act 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); Sandy Crank, *The Evolution of Privacy and Disclosure Policy in the Social Security Administration*, Soc. Sec. Bull., Jun. 1985, at 9. Current SSA regulations continue this tradition of safeguarding *all* SSA records and information, however officially acquired, including SSNs. *See* 42 U.S.C. § 1306(a); 20 C.F.R. §§ 401.5-401.95 (implements the Privacy Act of 1974, *infra* Section I.B).

The SSA has not only incorporated the safeguarding of information into its own policy manual, it has spoken specifically about disclosures to DHS, stating unequivocally that SSA "does not have the legal authority to disclose information

about U.S. citizens to DHS." Soc. Sec. Admin., POMS GN 03325.002, Disclosure and Verification of Social Security Numbers (SSN) Without Consent (2023).

Indeed, 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. *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.

B. The Privacy Act of 1974 Responded Directly to the Threat of the SSN Becoming a Universal Identifier and Restricted Its Disclosure

By 1974, the uses of SSNs had evolved far beyond their original purpose. Banks used them for tax reporting. The military used them as a service identification number. State agencies used them for driver's licenses, welfare programs, and tax administration. Congress recognized that this proliferation posed a fundamental threat to privacy and, in response, enacted the Privacy Act of 1974 (Privacy Act). 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).

During the course of hearings by the Committee on Government Operations' *ad hoc* Subcommittee on Privacy and Information Systems in June 1974 regarding

S. 3418, which became the Privacy Act, Senator Sam Ervin (D-NC) discussed the need for the passage of the bill:

> It is a rare person who has escaped the quest of modern government for information. Complaints which have come to the Constitutional Rights Subcommittee and to Congress over the course of several administrations show that, *this is a bipartisan issue which effects [sic] 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 make 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.*

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, the Committee heard from Arthur R. Miller, a distinguished Harvard Law School professor with widely recognized expertise in privacy, computers, and technology. Professor Miller warned of the "spread of the databank concept" in these prophetic terms:

> Americans today are scrutinized, measured, watched, counted, and interrogated by more governmental agencies, law enforcement officials, social scientists and poll takers than at any other time in our history. Probably in no Nation on earth is as much individualized information collected, recorded and disseminated as in the United States.
>
> *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*.
>
> * * *
>
> I think if one reads Orwell and Huxley carefully, one realizes that "1984" is a state of mind. In the past, dictatorships always have come with hobnailed boots and tanks and machineguns, 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.*

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

Senator Henry M. "Scoop" Jackson (D-Wash) expressed similar fears during the same debate: "[w]e 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 and I share that."[1] *Id.* at 57.

The SAVE overhaul represents precisely the type of centralized database that experts warned about and Congress feared when it enacted the Privacy Act. With its overhaul of the SAVE database, DHS is attempting to compile a massive records system that poses precisely the danger that Congress sought to prevent.

Further, the Privacy Act, by its terms, requires that, with closely circumscribed exceptions, agencies maintaining records on persons may not disclose that information "except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." 5 U.S.C. § 552a (b). Even with respect to the enumerated exceptions in which pre-authorization is not required prior to disclosure, agencies are required to maintain accurate accountings of the "date, nature, and purpose of each disclosure of a record to any person or to another agency" and "the name and address of the person or agency to whom disclosure is made." 5 U.S.C. § 552a (c)(1)(A) and (B). Each agency must also provide any person who so requests with access to his or her records and any information pertaining to

[1] *See also State ex rel. Beacon Journal Publishing Co. v. Akron*, 70 Ohio St.3d 605, 609-12 (1994) (recognizing that the purpose of the Privacy Act was "to curtail the expanding use of social security numbers by federal and local agencies and, by so doing, to eliminate the threat to individual privacy and confidentiality of information posed by common numerical identifiers").

him or her. 5 U.S.C. § 552a (d)(1). This would necessarily include the accounting of disclosures of that information.

C. Existing Statutory Frameworks Authorize the Disclosure of SSA Data to DHS Only for Narrow, Specific Purposes

Where Congress has chosen to authorize SSA disclosures to DHS, it has done so very carefully, specifying what data may be shared, the purpose for which this may occur, and whose data may be disclosed. In every case, laws that authorize disclosure—which fall under SSA regulation disclosures "required by law"—are much more narrowly drawn than the scope of the SAVE overhaul.

For example, the Immigration and Nationality Act (INA) requires SSA to disclose to DHS "information concerning the identity and location of *aliens* in the United States" when requested. 8 U.S.C. § 1360(b) (emphasis added). SSA's implementing guidance makes plain that the agency "may only disclose SSA information that will help DHS identify and or locate aliens in the United States." Soc. Sec. Admin., POMS GN 03313.095, Disclosure to the Department of Homeland Security (DHS) (2025). Two features of this authorization are critical. First, the statute is limited to *aliens*. There is no authority under the INA to collect, verify, or disclose SSA information about *U.S. citizens* to DHS. 8 U.S.C. § 1373(c). Second, the SSN may only be disclosed for *verification* purposes—that is, to confirm that DHS has the right individual for purposes of locating an alien. *Id*. The INA

does not authorize SSA to feed SSNs and citizenship data into a bulk processing system for the purpose of checking voter eligibility.

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 authorizes 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 name and address of the employer, and the amount of earnings. *Id*. It certainly does not allow disclosure of groups of people or non-aliens.

The Help America Vote Act of 2002 (HAVA) provides that state election boards may verify voter eligibility with SSA, but only as a secondary source when the state cannot verify registration information through state motor vehicle agency records. 52 U.S.C. § 20507. Even then, the verification uses only the last four digits of the SSN. 52 U.S.C. § 21083(a)(5)(B). The HAVA does not authorize the disclosure of SSA information to DHS.

Defendants invoke 8 U.S.C. § 1373 as statutory authority for the SAVE overhaul. As Plaintiffs correctly demonstrate, § 1373 is a *prohibitory* statute that does not affirmatively grant disclosure authority. *See* Memorandum in Support of Plaintiffs' Motion for Summary Judgment, ECF No. 61-1, pp. 39-42 of 63. Even setting aside that threshold problem, § 1373 is silent as to SSNs and SSA records,

and it certainly does not permit bulk data matching. It addresses "citizenship or immigration status" information held by DHS. 8 U.S.C. § 1373. It does not authorize DHS to reach into SSA's databases and extract SSNs, names, dates of birth, death indicators, and citizenship codes for hundreds of millions of Americans. To read the statute as authorizing the massive disclosure of sensitive personal information that is at issue in this case is flatly inconsistent with the Congressional solicitude for the confidentiality of this information described above.

D. Congress has Historically Allowed the Sharing of SSNs with Other Federal Agencies in Only Limited Contexts

The legislative record since the passage of the Privacy Act underscores Congress's understanding of its role in authorizing any new uses of SSNs. While Congress has legislated new SSN disclosure authorizations since 1976, it has done so narrowly and specifically. And it has largely done so in contexts related to providing federal benefits to qualified individuals. The following examples of disclosures permitted by Congress are illustrative rather than exhaustive.

In 1976, Congress amended the Social Security Act to allow states to use SSNs in accordance with four specifically authorized purposes: the administration of taxation; public assistance; driver's license registration; and motor vehicle registration. Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520. In addition to the authorization of SSN disclosure, the amendments included language that made

unlawful disclosure or compelled disclosure of SSNs a felony under federal law and the misuse of SSNs a violation of the Social Security Act. *Id*.

A year later, in keeping with the SSN's connection to the provision of benefits, Congress required SSN disclosure as a condition of eligibility for the food stamp program. Similarly, in 1981, it required SSN disclosure by adult members of a household with children applying for the school lunch program. Pub. L. No. 96-58, 93 Stat. 389; Omnibus Budget Reconciliation Act of 1981, Pub. L. No. 97-35, 95 Stat. 357. Congress also authorized the disclosure of the name and SSN of prisoners convicted of a felony to the Secretary of Health and Human Services to ensure suspension of disability benefits during incarceration. Social Security Amendments of 1981, Pub. L. No. 97-123, 95 Stat. 1659. Again, these disclosures are specifically related to ensuring that federal benefits are provided only to qualified individuals.

The Deficit Reduction Act of 1984 amended the Social Security Act again to establish an income and eligibility verification system for state agencies administering the Aid to Families with Dependent Children (AFDC) program, Medicaid, unemployment compensation, and food stamps. Deficit Reduction Act of 1984, Pub. L. No. 98-369, 98 Stat. 494. Congress specifically authorized states to require SSNs as a condition for eligibility in these programs if they chose to do so. *Id*.

Federal legislation in 1986 authorized the disclosure of SSNs in several specific situations. For example: SSNs were included on tax returns for dependents older than five; the Secretary of Transportation could require the use of SSNs on motor vehicle operators' licenses; and student loan applicants were required to report their SSNs as a condition of eligibility for an education loan. Tax Reform Act of 1986, Pub. L. No. 99-514, 100 Stat. 2085; Commercial Motor Vehicle Safety Act of 1986, Pub. L. No. 99-570, tit. XII, 100 Stat. 3207-170; Higher Education Amendments of 1986, Pub. L. No. 99-498, 100 Stat. 1268. In 1988, Congress passed a statute that authorized a state or any blood donation facility to use SSNs for identification of blood donors. Technical and Miscellaneous Revenue Act of 1988, Pub. L. No. 100-647, 102 Stat. 3342. These and other examples that we have not described here all are carefully tailored authorizations for disclosure of information only when it is directly relevant to the specific purpose for which disclosure is permitted.

II. Sharing of SSNs Under SAVE Is Unwarranted Because the SSA Does Not Have Accurate Records of Who Is a United States Citizen

The government's action at issue in this case is contrary to the limited circumstances in which Congress has authorized disclosure of information because SSNs are not an accurate source of information about citizenship status. DHS is the entity that has the most up-to-date and accurate immigration and citizenship status information on those who are not natural-born citizens, as well as those who have

been processed by the immigration system. In contrast, SSA's records are not accurate when it comes to citizenship status. The purpose of SSA records is to track eligibility for SSA benefits, not citizenship status. Because individuals only interact with the SSA to obtain an SSN for work purposes or to apply for benefits, SSA records regarding citizenship status reflect status only at that time, not an individual's current status. A person may not be a citizen at the time of applying for an SSN but may become one at a later point without SSA updating citizenship information. The reliance on SSA records to assess citizenship status therefore is not only unlawful but unlikely to provide information that is accurate for the purpose for which DHS ostensibly seeks it.

Indeed, the SSA's Office of the General Counsel has conceded that its own records should not be relied upon to determine U.S. citizenship: "While SSA records provide an indication of citizenship, they do not provide definitive information on U.S. citizenship." 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. When people apply for their SSNs, they report their citizenship status at that time. *Id*. The SSA does not make determinations about U.S. citizenship. *Id*.

Further, it was not until 1981 that the SSA began "to consistently maintain citizenship information. . ." *Id.* As a result, the SSA "does not have citizenship information for all individuals who have been issued an SSN." *Id.* Nor is an individual obliged to update his or her citizenship status with SSA unless the individual receives Social Security benefits or requests a replacement card. *Id.* Thus, "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." *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 the foreign-born U.S. citizens and non-U.S. citizens." 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. The IG reviewed SSA records and concluded that 7.0% of the people identified as non-U.S. citizens were actually U.S. citizens. *Id.* at 13. According to that study, "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.*

In sum, SSA's database is not a reliable source of information on who is a U.S. citizen, particularly when it comes to naturalized citizens. There is therefore no reason for personal information from SSA's files to be shared with DHS or to be included in the SAVE database.

DHS added SSA records to the SAVE database as part of the federal government's unilateral overhaul purportedly to convert it into a database to verify immigration and U.S. citizenship status. Press Release, Dep't of Homeland Sec., DHS, USCIS, DOGE Overhaul Systematic Alien Verification for Entitlements Database (Apr. 22, 2025), https://www.dhs.gov/news/2025/04/22/dhs-uscis-doge-overhaul-systematic-alien-verification-entitlements-database; [https://perma.cc/5R4V-4G2B].

Yet these records included the SSNs of foreign-born and U.S.-born citizens alike. Not only is it illegal to share confidential information without Congressional authorization, there is no reason for the records of natural-born U.S. citizen to be in the hands of immigration authorities. Indeed, providing U.S. citizen records to immigration authorities directly contradicts SSA Regulation 1 and its progeny as well as the Act itself.

III. Courts Have Rejected Federal Efforts to Use Confidential SSNs to Purportedly Prevent Voter Fraud

Even if the SAVE overhaul were otherwise lawful—and it is not—sharing SSNs is not necessary to accomplish the federal government's stated objective of

preventing voter fraud. Courts have squarely addressed and rejected the argument for using SSNs for this purpose. Moreover, they have expressed general concern about gathering sensitive SSA information, as well as the government's motivations to consolidate it. The reason for creating a nationwide database with confidential SSNs is unclear, but may include efforts to deprive citizens of their right to vote, to violate privacy rights, or to support deportation activities.

The risks of this are reflected in the Department of Justice (DOJ) request that at least 47 states and Washington D.C. provide it with complete unredacted voter registrations lists. Some states have provided or agreed to provide their lists, including SSNs. As set forth in the Memorandum in Support of Plaintiffs' Motion for Summary Judgment, the sharing of SSA data has resulted in some Texans improperly being removed from voter rolls and being disenfranchised in the March 2026 primary. ECF No. 61-1, pp. 29-31 of 63.

Many states have refused to share unredacted voter rolls with the federal government and the latter has filed lawsuits attempting to compel states to do so. For example, in *United States v. Weber*, _ F. Supp. 3d _, 2026 WL 118807 (C.D. Cal. Jan. 15, 2026), the DOJ filed suit to compel California to produce the state's unredacted voter registration lists, citing the National Voter Registration Act (NVRA), HAVA, and other statutes. The Court granted California's motion to dismiss the complaint. *Id.* at *1. The Court criticized the DOJ for representing that

it sought sensitive voter information for "voter roll maintenance enforcement and compliance." *Id*. at *10. Rather, it said, the DOJ appears to be "on a nationwide quest to gather the sensitive, private information of millions of American for use in a centralized federal database" and perhaps for immigration enforcement activities. *Id*.

The Court in *Weber* also expressed its concern over the federal government's attempt to consolidate sensitive personal information: "Viewing the DOJ's campaign to collect sensitive voter data in the context of these agreements for other types of personal information paints an alarming picture regarding the centralization of Americans' information within the Executive Branch—without approval from Congress or Americans themselves." *Id*. at *11. The Court "does not take lightly DOJ's obfuscation of its true motives in the present matter." *Id*. at *12. It continued: "Congress passed the NVRA, Civil Rights Act, and HAVA to protect voting rights. If the DOJ wants to instead use these statutes for more than their stated purpose, circumventing the authority granted to them by Congress, it cannot do so under the guise of a pretextual investigative purpose." *Id*.

Another court has been troubled by the federal government's efforts to create a comprehensive database that includes social security numbers. In *United States v. Oregon*, 2026 WL 318402 (D. Or. Feb. 5, 2026), the U.S. government challenged the state's refusal to provide unredacted voter registration lists. The Court granted

Oregon's motion to dismiss the complaint. It warned that the federal government's "statements that it intends to create a nationwide database of confidential voter information and use it in unprecedented ways, including immigration enforcement efforts, is chilling." *Id.* at *13. It continued: "[t]he possibility that Oregon's voter registration list could be used to further these efforts in the absence of congressional action, may very well lead to an erosion of voting rights and voter participation." *Id*.

The SAVE overhaul inflicts the same type of harms and raises some of the same red flags as discussed by the courts in *Weber* and *Oregon*, *supra,* but on an exponentially larger scale. The federal government now seeks to consolidate and capture all the SSNs from state voter rolls, transmit them to SSA for bulk matching, and return citizenship data to state agencies, all without the knowledge or consent of the individuals involved.

IV. Centralizing and Consolidating SSNs in a Single National Database Creates Significant Security Risks

The federal government classifies any full or partial SSN as Personally Identifiable Information that increases identity theft risk. 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). The Government Accountability Office (GAO) has reported that SSNs, along with names and dates of birth, are "among the three personal identifiers most often sought by identity thieves." U.S. Gov't Accountability Office, Social Security

Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards, GAO-05-59, at 3 (Nov. 9, 2004). The end result of the overhaul of the SAVE database—a single consolidated national database with multiple millions of social security numbers—would be extremely vulnerable to cybersecurity attacks and widescale identity theft.

The practice of compartmentation—segregating data so that only those with a legitimate need have access—is a bedrock of information security. *See* Barbara McQuade, *Comment: DOJ's voter info demand a data breach waiting to happen* (Jan. 13, 2026), https://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), https://www.databank.com/resources/blogs/understanding-the-importance-of-data-segregation-and-access-control/. As one former national security prosecutor has observed, centralized databases create single points of failure: "A single breach of a database that contains both driver's license and Social Security numbers could enable identity theft on a massive scale." Barbara McQuade, *Comment, supra.*

The SAVE overhaul does the opposite of compartmentation and ignores the real security risks created by consolidating all SSNs of millions of Americans.

The risk of widescale identity theft is not merely theoretical. In 2024, the Identity Theft Resource Center documented 1,857 data breaches involving

Americans' SSNs. Kevin Collier, *Social Security Number Leaked? Chances Are, a Criminal is Already Trying to Use It*, ABC (Aug. 4, 2025), https://www.nbcnews.com/tech/security/security-numbers-leaked-personal-data-puts-people-high-risk-identity-rcna221452. The Federal Trade Commission received 1.1 million identity theft claims that year. *Id.* In January 2026, researchers detected an exposed database containing approximately 2.7 billion records containing Social Security numbers. Greg Pollock, *Social Insecurity: Billions of Social Security Number and Passwords*, UpGuard (Feb. 18, 2026), https://www.upguard.com/breaches/social-insecurity-billions-of-social-security-number-and-passwords. Federal systems themselves have been compromised: in August 2025, the federal court filing system was hit by a sweeping hack, and in December 2025, government contractors were charged in an insider data breach affecting multiple federal agencies. 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).

It is no secret that foreign adversaries and others have already attempted to hack, and sometimes have succeeded in hacking, U.S. government systems. *See* Cong. Rsch. Serv., R46974, Cybersecurity: Selected Cyberattacks, 2012–2024 (Jan. 8, 2025), https://www.congress.gov/crs-product/R46974; [https://perma.cc/9ED8-JE9K]; U.S. Gov't Accountability Office, GAO-17-614, Information Security: OPM Has Improved Controls, but Further Efforts Are Needed (Aug. 3, 2017), https://www.gao.gov/products/gao-17-614; [https://perma.cc/S65U-8GAR]; *Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls Across Federal Agencies: Testimony Before the Subcomm. on Cybersecurity, Infrastructure Prot., and Sec. Techs., H. Comm. on Homeland Sec.*, GAO-15-725T (statement of Gregory C. Wilshusen, Dir., Info. Sec. Issues, U.S. Gov't Accountability Office) (June 24, 2015).

A centralized database will inevitably be targeted by cybersecurity attacks and thus will needlessly expose the personal information of millions of people to theft and other misuse.

V. DOGE's Failure to Safeguard Confidential SSA Personal Information Illustrates the Risk of Widespread Disclosure of SSNs

There have been numerous reports of security breaches regarding SSA data since the Administration began its effort to overhaul the SAVE system. Not only

have several whistleblowers come forward to report the Department of Government Efficiency's (DOGE) mishandling of SSA Numident data, but the DOJ itself acknowledges that some DOGE employees failed to safeguard this information.

For example, in August 2025, SSA's former chief data officer, Charles Borges, came forward to report security lapses by DOGE. He has alleged that DOGE members improperly uploaded copies of SSA personal information to a digital cloud, thus placing this confidential information at risk. 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, *et al*. (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.

The SSA's Inspector General apparently is also investigating a whistleblower claim that a former DOGE member sought to download the SSA Numident database to a thumb drive so that he could transfer the data and use that information at his new job. 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.

Moreover, the DOJ acknowledges breaches by DOGE. From March 7, 2025, through March 17, 2025, "members of SSA's DOGE Team were using links to share data through the third-party server 'Cloudfare,'" which "is not approved for storing SSA data and when used in this manner is outside SSA's security protocols." *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. The DOJ concedes that it does not know "exactly what data were shared to Cloudflare or whether the data still exist on the server." *Id*.

In addition, the DOJ reports that a "political advocacy group" (which the DOJ declined to identify) reached out to two members of the SSA DOGE team "with a request to analyze state voter rolls that the advocacy group had acquired." *Id.* at 5. The advocacy group's "stated aim was to find evidence of voter fraud and to overturn election results in certain States." *Id*. A DOGE team member went so far as to sign a "'Voter Data Agreement,' in his capacity as an SSA employee, with the advocacy group" and sent "the executed agreement to the advocacy group on March 24, 2025." *Id*. This advocacy group may have asked the DOGE team members to "access[] SSA data to match to the voter rolls," but the "SSA has not yet seen evidence that SSA data were shared with the advocacy group." *Id.* at fn. 1. At the same time, the

SSA has not specifically ruled out that its data may have been shared with this advocacy group. *Id.* at 6.

CONCLUSION

The overhaul of the Systemic Alien Verification Database through the integration of SSNs that was initiated by Executive Order 14248 is unauthorized by law. It is directly contrary to decades of Congressional and administrative efforts to ensure that SSNs are disclosed only for limited specific purposes that the provision of this information will serve. The government's action at issue in this case attempts to create the type of centralized nationwide database of highly sensitive personal information that poses grave risks to democracy and individual liberty.

Respectfully submitted,

/s/ Aderson B. Francois
Aderson B. Francois, Esq.
(D.C. Bar No. 498544)
Civil Rights Clinic
Georgetown University Law Center
600 New Jersey Ave., NW
Washington, DC 20001
Phone: (202) 661-6721
Fax: (202) 662-9634
aderson.francois@georgetown.edu

Counsel of record for
Lawyers Defending
American Democracy

CERTIFICATE REQUIRED BY LCvR 26.1 OF THE LOCAL RULES OF THE UNITED STATES DICTRICT COURT FOR THE DISTRICT OF COLUMBIA

I, the undersigned counsel of record for *Amicus Curiae* Lawyers Defending American Democracy, certify that Lawyers Defending American Democracy is a non-partisan tax exempt 501(c)(3) corporation. Amicus is not owned by any parent corporation, and no publicly held company has 10% or more ownership in LDAD.

These representations are made in order that judges of this Court may determine the need for recusal.

/s/ Aderson B. Francois
Aderson Francois, Esq.
Counsel of Record for
Lawyers Defending
American Democracy

CERTIFICATE OF SERVICE

I certify that on March 30th, 2026, this brief was filed using the Court's CM/ECF system. All participants in the case are registered CM/ECF users and will be served electronically via that system.

/s/ Aderson B. Francois
Aderson B. Francois, Esq.
Counsel of Record for
Lawyers Defending
American Democracy